MASTER'S THESIS

De impact van factoren van privacy beleid op consumentenvertrouwen in e-commerce

Hijum, J. (Jony)

Award date:
2020

De impact van factoren van privacy beleid op consumentenvertrouwen in e-commerce

The impact of privacy policy factors on consumer trust in e-commerce

Opleiding:	Open Universiteit, faculteit Bètawetenschappen Masteropleiding Business Process Management & IT
Cursus:	IM0602 BPMIT Graduation Assignment Preparation IM9806 Business Process Management and IT Graduation Assignment
Student:	Jony van Hijum
Student ID:	
Datum:	24 juni 2020
Scriptie supervisor:	Dr. Laury Bollen
Tweede lezer:	Dr. Rachelle Bosua
Versie:	1.0
Status:	~~concept~~ / definitief

Abstract

A recent report from the Dutch Data Protection Authority shows that consumers don't always trust online web shops when it comes to their privacy. Previous studies found a connection between consumer trust and the willingness to buy products from an organization. Therefore, it is important to know which factors raise consumer trust in the context of privacy. The objective of this research is to investigate the impact of several privacy policy factors on consumer trust in the context of e-commerce. The influencing factors this study is particularly focusing at, are data protection officer (DPO), privacy policy and trustmark. According to the results, a good privacy policy and a visible trustmark have a positive influence on consumer trust. For having a good DPO, there was no significance found that it influences consumers' trust. Another result that was found, is that the more factors a company applies, the more a consumer trusts that organization, especially when it comes to a visible trustmark and a good privacy policy. The research field of a DPO in relation to consumer trust is relatively new. Future research could focus therefore particularly on this factor.

Key words

E-commerce, consumer trust, data protection officer, privacy policy, trustmark

Samenvatting

Met de komst van computers, tablets, smartphones is de hoeveelheid data die van de consument wordt verkregen, enorm toegenomen. Deze data kan gemakkelijk worden opgeslagen en verzameld met behulp van nieuwe ontwikkelingen en technologieën. Het verwerken van persoonsgegevens brengt risico's met zich mee voor de consument maar tegelijkertijd is het verkrijgen van deze data voor bedrijven heel belangrijk.

Een rapport van de Autoriteit Persoonsgegevens uit 2019 toont aan dat 87% van de Nederlanders zich nog steeds veel zorgen tot zeer veel zorgen maakt over de manier waarop hun persoonsgegevens worden verwerkt door online winkels en dat ze er soms zelfs wantrouwend tegenover staan. Tegelijkertijd laten verschillende onderzoeken zien dat wanneer consumenten een webwinkel vertrouwen, ze eerder bereid zijn tot het doen van aankopen, ze eventueel terugkomen voor her-aankopen en dat leidt uiteindelijk tot meer omzet. Wanneer online bedrijven dus weten welke factoren van privacy beleid bijdragen aan een verhoogde vertrouwensperceptie, dan loont het om daarin te investeren. De hoofdvraag van dit onderzoek luidt daarom: *Wat is de invloed van het privacy beleid van online bedrijven op de vertrouwensperceptie van consumenten?*

Om de hoofdvraag te kunnen beantwoorden zijn er een drietal elementen bekeken die organisaties toe kunnen passen in hun privacy beleid namelijk een goede privacy policy, het tonen van een privacy keurmerk en het aanstellen van een goede Data Protection Officer (Functionaris Gegevensbescherming). In een enquête onder 81 respondenten zijn er random verschillende scenario's voorgelegd waarbij van ieder element ofwel een goede variant is getoond ofwel een minder goede variant is getoond. Vervolgens kregen alle respondenten dezelfde vragen over hun vertrouwen in deze (fictieve) casus organisatie.

Uit de resultaten blijkt dat een goede privacy policy en het tonen van een keurmerk een positieve invloed heeft op het vertrouwen van consumenten. Een goede Data Protection Officer draagt niet bij aan een verhoogd vertrouwen van consumenten in organisaties. Ook blijkt dat het gecombineerd tonen van elementen kan leiden tot meer vertrouwen dan wanneer elementen los worden getoond. Hierbij geldt dat hoe meer goede elementen worden getoond, hoe meer het vertrouwen stijgt en dat vooral het toevoegen van een goede privacy policy en het tonen van een keurmerk bovenop een losstaand element, van toegevoegde waarde kan zijn.

Een belangrijke beperking van dit onderzoek is dat er al literatuur bestaat over een keurmerk en een privacy policy in relatie tot vertrouwen waarop dit onderzoek voor een deel is gebaseerd. Over een Data Protection Officer is deze literatuur nog niet beschikbaar, vermoedelijk omdat het een relatief nieuwe functie is. Vervolgonderzoek is nodig om deze relatie verder te onderzoeken zodat bijvoorbeeld bepaald kan worden wat überhaupt wordt verstaan onder een goede DPO.

Summary

With the raising usage of computers, tablets, smartphones, the amount of data obtained from the consumer has increased enormously. This data can be easily stored and collected using new developments and technologies. Processing personal data entails risks for the consumer but is very important for companies.

A report by the Dutch Data Protection Authority from 2019 shows that 87% of Dutch people are still very much concerned to very much concerned about the way their personal data are processed by online stores and that they are sometimes even suspicious of it. At the same time, several studies indicate that when consumers trust an online web shop, they feel more comfortable make purchases, they may even come back for re-purchases and that ultimately leads to more sales. So, when online companies know which factors of privacy policy contribute to an increased perception of trust, they can invest in it. The main question of this study is therefore: *What is the influence of the privacy policy of online companies on the perception of consumer confidence?*

In order to answer the main question, three elements have been examined that organizations can apply in their privacy policy, namely a good privacy policy, showing a privacy trustmark and appointing a good Data Protection Officer (DPO). In a survey of 81 respondents, random scenarios were presented in which from each element is shown either a good variant or a less good variant. All respondents were then asked the same questions about their trust in this (fictitious) case organization.

The results show that a good privacy policy and showing a trustmark have a positive influence on consumer trust. A good Data Protection Officer does not contribute to increased consumer trust in organizations. It also appears that showing a combination of elements can lead to more confidence than when elements are shown separately. The more good elements are shown, the more trust increases and especially the addition of a good privacy policy and the display of a trustmark on top of a separate element can be of added value.

An important limitation of this study is that there was already literature about a trustmark and a good privacy policy in relation to trust on which this research is partly based. This literature is not yet available on a Data Protection Officer, presumably because it is a relatively new position. Follow-up research is needed to further investigate this relationship.

Inhoudsopgave

Overzicht van figuren

Overzicht van tabellen

1. Inleiding

Met de komst van computers, tablets, smartphones is de hoeveelheid data die van de consument wordt verkregen, enorm toegenomen (Simpson, 2016). Deze data kan gemakkelijk worden opgeslagen en verzameld met behulp van nieuwe ontwikkelingen en technologieën (Pelteret & Ophoff, 2016). Consumenten staan echter wantrouwend tegenover deze ontwikkelingen wanneer er wordt gekeken naar de manier waarop bedrijven omgegaan met hun privacy. De Autoriteit Persoonsgegevens heeft namelijk recent onderzocht dat 87% van de Nederlanders zich nog steeds veel zorgen tot zeer veel zorgen maakt over hun privacy. Dit rapport laat verder zien dat consumenten vooral wantrouwend staan ten opzichte van webwinkels en de manier waarop zij de persoonsgegevens verwerken van hun klanten (Autoriteit Persoonsgegevens, 2019c). Uit onderzoek blijk dat deze zorgen niet geheel onterecht zijn. Jayasinghe, Lee, en MacDermott (2018) hebben onderzocht dat zodra iemand gebruikmaakt van onlinediensten, hij of zij daarmee ook persoonsgegevens verstrekt aan de aanbieder van deze dienst. En voor consumenten brengt dat risico's met zich mee (De & Métayer, 2016). Deze risico's zijn bijvoorbeeld het stelen van iemands identiteit (Gellman & Dixon, 2011) of omdat de gegevens worden gebruikt voor profiling (Abedjan, Golab, & Naumann, 2015). Tegelijkertijd is het voor bedrijven wel heel belangrijk dat consumenten bereid zijn om persoonsgegevens te delen (Vance, 2009). Door deze data krijgen bedrijven inzage in hun klanten, de markt of gedetailleerde informatie over aankoophistorie (Verhoef, Kooge, & Walk, 2016). Dit zorgt ervoor dat bedrijven beter in staat zijn om beslissingen te nemen en de consument beter van dienst zijn. Ook laten verschillende onderzoeken zien, waaronder die van Reichheld en Schefter (2000), Van Dyke, Midha, en Nemati (2007), Harris en Goode (2004) en Sullivan en Kim (2018), dat wanneer consumenten vertrouwen hebben in een online organisatie, ze eerder bereid zijn tot het doen van aankopen, ze eventueel terugkomen voor her-aankopen en dat leidt uiteindelijk tot meer omzet voor een organisatie. Hierdoor is het voor bedrijven interessant om te weten welke middelen zij kunnen inzetten in de context van de AVG, om het vertrouwen van de consument in hun organisatie te vergroten.

1.1 Noodzaak van de AVG

Omdat dit onderzoek plaatsvindt in de context van de AVG, is het belangrijk om te begrijpen hoe de AVG ontstaan is en welk doel het dient. In deze paragraaf wordt hier dieper op ingegaan.

Na vele jaren van onderhandeling, lobbyen en schrijven is op 27 april 2016 de definitieve tekst voor de *Algemene verordening gegevensbescherming* (AVG) gepubliceerd. Na publicatie volgde een tweejarig implementatieprogramma waarna de AVG op 25 mei 2018 van kracht is geworden (EDPS, 2016). De AVG is een Europese verordening die de bescherming van een belangrijk grondrecht regelt, namelijk de bescherming van persoonsgegevens. Een verordening is een Europese wet en is van kracht voor alle lidstaten van de EU. Dit in tegenstelling tot een richtlijn, die eerst naar nationaal recht moet worden omgezet (Schermer, Hagenauw, & Falot, 2018). Er is dus niet zoiets als een Nederlandse implementatie van de verordening, er is wel sprake van een naar het Nederlandse vertaalde versie. De verordening is dus gelijk voor alle lidstaten van de Europese Unie (Schermer et al., 2018). De AVG is de eerste verordening die door de Europese Unie aan de lidstaten is opgelegd. De AVG vervangt daardoor de in 1995 gepubliceerde Data protectie richtlijn. Zoals de naam al aangeeft, betrof dit een richtlijn waardoor er in de vertaling hiervan naar nationale wetten

veel ruimte was voor interpretatie door de verschillende lidstaten. Daarnaast was de richtlijn uit 1995 gedateerd door de technologische veranderingen van de afgelopen jaren (Schermer et al., 2018). De AVG is dus voornamelijk van kracht geworden om de wetten die reeds bestonden in de EU-landen over hoe er werd omgegaan met persoonsgegevens, in de gehele EU, gelijk te trekken. Daarmee hebben inwoners meer zeggenschap gekregen over hun gegevens en worden persoonsgegevens beter beschermend (Ayala-Rivera & Pasquale, 2018). Daarnaast geldt de AVG voor alle bedrijven die actief zijn in Europa. Het maakt hierbij niet uit of er sprake is van onlinedata of offlinedata, of gegevens automatisch of handmatig worden verwerkt, of het bedrijf groot is of klein, of dat het bedrijf binnen of buiten Europa is gevestigd. Zolang een bedrijf actief is in Europa, geldt de AVG (Axinte, Petrică, & Bacivarov, 2018).

1.2 Privacy en databescherming

Omdat AVG en privacy sterk met elkaar verbonden zijn, is het ook belangrijk om helder te krijgen wat het begrip privacy precies betekent. Allereerst wordt privacy vooral gebruikt als definitie voor uiteenlopende zaken zoals de controle over persoonlijke informatie, het wel of niet hebben van toegang tot plekken, geheimhouding of reproductieve autonomie. Daarnaast is het ook per cultuur verschillend wat er onder privacy wordt verstaan. Iets waar de wetenschap het over eens is, is dat privacy voorkomt in iedere cultuur (Roberts & Gregor, 2017; Westin, 1968). In de Europese wet is er een verschil tussen privacy en databescherming maar worden ze vaak samen genoemd. Dit maakt dat deze twee concepten dicht bij elkaar liggen, maar niet als hetzelfde kunnen worden gezien. Privacy refereert in deze context vaak aan de bescherming van iemand zijn/haar persoonlijke omgeving, terwijl databescherming gaat over beperkingen of voorwaarden voor het gebruik van data van een individu. Juridisch gezien zijn privacy en databescherming dus twee verschillende, maar fundamentele rechten in het Europese recht. Privacy wordt gezien als een substantieel recht, terwijl databescherming meer wordt gezien als procedureel recht (Politou, Alepis, & Patsakis, 2018). Ondanks dat er een verschil is tussen privacy en databescherming, laat privacy zich als term moeilijk definiëren, blijkt uit onderzoek (Kemp, 2007). Het voor dit onderzoek minder van belang om een definitie van privacy te hebben maar het is wel belangrijk om te weten het begrip privacy zich lastig laat definieren.

1.3 Relevantie van dit onderzoek

Zoals eerder is aangegeven, blijkt uit onderzoek van de Autoriteit Persoonsgegevens dat consumenten wantrouwend tegenover webwinkels staan omdat ze zich zorgen maken over de manier waarop webwinkels hun persoonsgegevens verwerken (Autoriteit Persoonsgegevens, 2019c). Tegelijkertijd is met de komst van de AVG ook een aantal maatregelen van kracht geworden die organisatie kunnen of soms wettelijk moeten toepassen in het kader van het omgaan met persoonsgegevens en de privacy van consumenten. Verschillende onderzoeken hebben echter aangetoond dat er een relatie is tussen vertrouwen en de mate waarin organisaties bereid zijn om te voldoen aan wetgeving. Met name de onderzoeken van Oliver (1991), Suchman (1995) en Mayer, Davis, en Schoorman (1995) leggen hiervoor een belangrijke basis.

Dit onderzoek richt zich op de invloed van verschillende privacy maatregelen en hun invloed op consumentenvertrouwen in webwinkels, in de context van de AVG. Een dergelijk onderzoek is niet helemaal nieuw. Door Wu, Huang, Yen, en Popova (2012) is bijvoorbeeld

onderzocht dat er een relatie is tussen vertrouwen en een online privacy policy. En door Liu, Marchewka, Lu, en Yu (2005) is onderzocht dat er een relatie is tussen het tonen van een privacy keurmerk en het vertrouwen van consumenten. Deze onderzoeken hebben echter allemaal plaatsgevonden binnen een andere context dan de AVG en hebben niet in Nederland plaatsgevonden. Bovendien hebben deze onderzoeken puur gekeken naar de elementen als losstaande concepten of in vergelijking met andere elementen. Ook blijkt dat lang niet alle elementen die vanuit de AVG toegepast kunnen worden al zijn onderzocht. Waar bijvoorbeeld nog geen onderzoek naar is gedaan, maar wat wel is gesuggereerd door Recio (2017), is of het aanstellen van een Functionaris Gegevensbescherming (Data Protection Officer) van invloed is op het vertrouwen van consumenten.

Dit onderzoek richt zich specifiek op de invloed van deze drie beleidsmaatregelen op het vertrouwen van Nederlandse consumenten in webwinkels, in de context van de AVG. Deze drie elementen worden gecombineerd aan respondenten voorgelegd in een enquête. Bovendien worden ze bij wijze van experiment getoond, waarbij er goede varianten zijn en minder goede varianten. Door ze te combineren kan er gekeken worden of een combinatie van bepaalde goede elementen versterkend werkt ten opzichte van losstaande elementen. De combinatie van deze drie elementen, het gecombineerd toetsen van deze elementen en het gebruik van een experiment als onderzoeksvorm, maken dit onderzoek uniek

1.3.1 Onderzoeksvraag

Op basis van een verkennende literatuurstudie is gezocht naar een invalshoek die nog niet eerder is onderzocht, maar wel wetenschappelijke relevantie heeft zoals hiervoor beschreven. Vervolgens is de volgende onderzoeksvraag geformuleerd:

> *Wat is de invloed van het privacy beleid van online bedrijven op de vertrouwensperceptie van consumenten?*

1.4 Opbouw rapport

In hoofdstuk 2 wordt besproken welke onderzoeken er reeds zijn gedaan op dit gebied, wat daarin is onderzocht en waarop dit onderzoek zich precies zicht. In hoofdstuk 3 wordt besproken hoe het onderzoek wordt uitgevoerd en welke afwegingen hierin zijn gemaakt. In hoofdstuk 4 worden de resultaten van het onderzoek besproken en worden er verschillende analyses uitgevoerd om verbanden te toetsen. In hoofdstuk 5 wordt de uitkomst van het onderzoek besproken en wordt er gereflecteerd op wat er beter had gekund. Ook worden hierin inzichten besproken voor vervolgonderzoek.

2. Theoretisch kader

Het theoretisch kader vormt de basis voor het onderzoek en heeft als doel om tot een onderbouwde set afhankelijke en onafhankelijke variabelen te komen. Voorafgaand aan het theoretisch kader is een zoekstrategie opgesteld. Deze is te vinden in bijlage 1.

2.1 Het gedrag van organisaties verklaren

Om te kunnen verklaren waarom organisaties bepaald beleid hanteren, in relatie tot wetgeving zoals de AVG, is het noodzakelijk om inzicht te krijgen in het gedrag van organisaties. De *institutionele theorie* en de *resource dependence theorie* proberen beiden de strategische reacties van organisaties op externe druk en verwachtingen te verklaren (Oliver, 1991). Waar beide theorieën het over eens zijn, is dat organisaties moeten reageren op druk en verwachtingen van buitenaf om te kunnen blijven voortbestaan (Meyer & Rowan, 1977). Daarnaast benadrukken beide theorieën het belang van het verkrijgen van legitimiteit voor organisaties om hun maatschappelijke waarde aan te kunnen tonen (Oliver, 1991). Het verschil tussen beide theorieën is te vinden in de manier waarop ze kijken naar de macht van de externe actoren (Oliver, 1991). Voor de *institutionele theorie* ligt de macht bij degene die de vorm van de institutionele regels bepaalt, voor de *resource dependence theorie* ligt de macht bij degene die de schaarse resources heeft. De *resource dependence theorie* verklaart het gedrag van organisaties vooral door middelen die organisaties nodig hebben van externe actoren om te kunnen blijven voortbestaan (Pfeffer & Salancik, 2003). De *institutionele theorie* richt zich vooral op de druk van instituties op organisaties als verklaring voor het gedrag van organisaties (Meyer & Rowan, 1977). De *institutionele theorie* baseert zich op het basisprincipe dat instituties gevoelig zijn voor sociale invloeden en druk, tradities en normen (Meyer & Rowan, 1977). Scott (1987) definieert instituties, zoals die in de institutionele theorie worden bedoeld, als overheidsorganisaties, wetten, rechtbanken en experts. Uit een onderzoek van Carpenter en Feroz (2001) blijkt vervolgens dat succesvolle organisaties in staat zijn om legitimiteit te verkrijgen door zich te laten beïnvloeden door sociale druk waarmee zij in hun onderzoek legitimiteit dus koppelen aan de institutionele theorie.

In het kader van dit onderzoek, zou de institutionele theorie het meest voor de hand liggen als uitgangspunt. Aangezien deze theorie zich richt op instituties als verklaring voor het gedrag van organisaties, is de relatie met de implementatie van de AVG als zijnde institutie hierdoor goed te leggen. Echter zou dat slechts een deel verklaren, namelijk dat organisaties de AVG implementeren. Het verklaart nog niet de mate van implementatie. Om dit verschil te kunnen verklaren is het noodzakelijk om nog een andere theorie te bestuderen, namelijk die van het belang van legitimiteit. Legitimiteit komt namelijk in beide theorieën terug als mogelijke verklarende factor voor de mate waarin beleid door organisaties wordt geïmplementeerd.

2.2 Legitimiteit van organisaties

Legitimiteit is een cruciale factor voor het voortbestaan en succes van organisaties, stelt Suchman (1995). Hiermee legt hij een basis voor de *'legitimacy theory'*. Hij hanteert de volgende definitie voor legitimiteit: *"Legitimacy is a generalized perception or assumption that the actions of an entity are desirable, proper, or appropriate within some socially constructed system of norms, values, beliefs, and definitions."* (Suchman, 1995).

In zijn onderzoek worden legitimiteit en de institutionele theorie aan elkaar gekoppeld. Ook in andere onderzoeken, zoals in die van Deephouse en Carter (2005) en Richardson en Joshi (1997), wordt geschreven over het belang van legitimiteit voor de institutionele theorie en de resource dependence theorie. Richardson en Joshi (1997) schrijven in hun onderzoek dat organisaties worden gezien als 'entiteiten' die liever legitimiteit willen nastreven dan maximale winst, in de context van de institutionele theorie. Volgens hun onderzoek wil een organisatie aan de ene kant bezig zijn met de eigen, individuele zoektocht naar winst en de wens om te overheersen. Maar aan de andere kant zijn organisaties nog meer bezig met het verkrijgen of vasthouden van legitimiteit. Suchman (1995) en Brown en Dacin (1997) schrijven in hun onderzoek dat organisaties die worden gezien als legitiem, beter in staat zijn om de beschikbare resources te bemachtigen en ongelimiteerde toegang hebben tot markten, wat allebei hun kans op voortbestaan vergroot.

Binnen de literatuur zijn drie soorten legitimiteit te definiëren, namelijk *pragmatic legitimacy*, *moral legitimacy (*of binnen de institutionele theorie ook wel *normative legitimiacy* genoemd*)* en *cognitive legitimacy* (Suchman, 1995). Alle drie de soorten legitimiteit hebben betrekking op een gegeneraliseerd idee dat organisatorische activiteiten wenselijk, gepast, of passend zijn binnen een sociaal geconstrueerd systeem van normen, waarden, overtuigingen en definities. Elk type legitimiteit berust echter op een iets andere gedragsdynamiek, schrijft Suchman (1995) in zijn artikel.

Pragmatic legitimacy houdt in dat legitimiteit wisselt tussen de organisatie en haar publiek. Een organisatie krijgt support van het publiek voor een bepaald beleid, gebaseerd op de verwachte waarde of betekenis wat dat beleid heeft voor het publiek (Wood, 1991).

Moral legitimacy berust niet op de beoordeling of een bepaalde activiteit het publiek ten goede komt, zoals bij pragmatic legitimacy het geval is, maar op het oordeel of de activiteiten van de organisatie 'de enige juiste zijn om te doen'. Deze oordelen weerspiegelen op hun beurt meestal de overtuiging of de activiteiten maatschappelijk welzijn bevorderen, zoals het door het publiek bepaald sociaal geconstrueerd waardesysteem (Aldrich & Fiol, 1994).

Cognitive legitimacy doet zich voor als er zo'n hoge mate van congruentie of acceptatie tussen de normatieve verwachtingen van de organisatie en haar publiek is, dat ze niet worden betwist maar meer als vanzelfsprekend of 'natuurlijk' worden ervaren (Hannan & Freeman, 1986).

Legitimiteit beïnvloed niet alleen hoe mensen zich gedragen ten opzichte van organisaties, maar ook hun beeld van de organisatie en daarmee dus de reputatie van organisaties (King & Whetten, 2008). Het gevolg hiervan is dat het publiek, legitieme organisaties niet alleen waardevoller, maar ook betekenisvoller, voorspelbaarder en betrouwbaarder acht (Suchman, 1995). Daar tegenover hebben organisaties, die weinig legitimiteit hebben opgebouwd bij het publiek, een grote kans om te worden gezien als irrationeel, onnodig en nalatig (Meyer & Rowan, 1977). Hieruit is op te maken dat legitimiteit van organisaties van invloed is op het vertrouwen van consumenten in organisaties.

2.3 Vertrouwen

Reichheld en Schefter (2000) schrijven in hun onderzoek dat vertrouwen van vitaal belang is voor klanten in de context van digitale klantrelaties. Vertrouwen leidt namelijk tot loyaliteit en wanneer consumenten, vertrouwen hebben in een online verkoper, dan zijn ze eerder bereid persoonsgegevens met deze partij te delen. Dit leidt ertoe dat webwinkels meer persoonlijk contact kunnen maken met klanten, bijvoorbeeld door ze persoonlijke aanbiedingen te doen, wat weer leidt tot meer vertrouwen. Vertrouwen blijkt zelfs nog belangrijker te zijn dan bijvoorbeeld een lage prijs (Reichheld & Schefter, 2000). Ondanks dat vertrouwen volgens de onderzoekers eigenlijk ook al van belang was in de tijd dat aankopen vooral offline werden gedaan, is vertrouwen juist voor webwinkels belangrijker dan ooit. Online klanten kunnen namelijk niet het product eerst aanraken of bekijken of een verkoopmedewerker in de ogen kijken (Reichheld & Schefter, 2000). Mayer et al. (1995) hebben onderzoek gedaan naar vertrouwen in organisaties en worden veel aangehaald als grondlegger in latere literatuur. Uit hun onderzoek blijkt dat er drie factoren zijn, ook wel *trusting beliefs* genoemd, die leiden tot vertrouwen namelijk ***ability***, ***benevolence*** en ***integrity*** met als overkoepelend concept ***propensity***. De mate van ability, benevolence en integrity zijn belangrijk voor vertrouwen en kunnen onafhankelijk van elkaar bekeken worden, maar zijn wel onlosmakelijk aan elkaar verbonden. Dat betekent dat wanneer een partij door een persoon op alle factoren hoog wordt gescoord, deze partij door die persoon als zeer betrouwbaar wordt gezien.

Propensity wil zeggen de algemene bereidheid om anderen te vertrouwen. Het heeft invloed op de mate van vertrouwen wat iemand heeft in een andere partij, nog voordat er meer informatie over die partij beschikbaar is. Propensity geeft eigenlijk de mate van 'blind vertrouwen' aan (Mayer et al., 1995). In paragraaf 2.3.2 wordt dit concept verder besproken.

Ability of ***competence based trust*** verwijst naar het vermogen van organisaties om beloften te realiseren. Deze beloften kunnen gerealiseerd worden wanneer de organisatie voldoende kennis, expertise, vaardigheden, leiderschap en andere kenmerken bezit voor het domein waarin ze actief zijn. Deze factor is dus domein specifiek, wat betekent dat een partij voor een bepaald domein wel het vertrouwen kan krijgen van iemand, maar in een ander domein mogelijk helemaal niet (Mayer et al., 1995).

Benevolence based trust is de mate waarin degene die het vertrouwen geeft, ervan uit gaat dat de partij die het vertrouwen krijgt, altijd het goede met hem/haar voorheeft en dat een economisch motief in mindere mate van belang is (Mayer et al., 1995). Dit is meer relevant voor een persoon tot persoon relatie, bijvoorbeeld de relatie tussen mentor en student, dan een persoon tot bedrijf relatie.

Integrity based trust houdt in dat degene die het vertrouwen geeft, de idee heeft dat de organisatie aan wie hij/zij het vertrouwen geeft, voldoet aan een aantal basisprincipes. Het suggereert dat een bedrijf op een consistente, betrouwbare en eerlijke manier handelt bij het vervullen van de beloften naar de consument (Mayer et al., 1995).

2.3.1 Factoren van vertrouwen als losstaande concepten

Later hebben P. Kim, Ferrin, Cooper, en Dirks (2004) voortgebouwd op het onderzoek van Mayer et al. (1995). In hun eigen onderzoek hebben ze ook gekeken naar vertrouwen, maar

vertrouwen werd dan niet gevormd door alle factoren, maar slechts door een selectie. In hun geval werd vertrouwen gevormd door ability-trust en integrity-trust. Uit het onderzoek blijkt dat als je kijk naar vertrouwen, het inderdaad niet altijd noodzakelijk is om naar alle drie de factoren gezamenlijk te kijken, maar dat je ook kunt kijken naar een of meerdere factoren die dan gezamenlijk vertrouwen vormen. Afhankelijk van het onderwerp van het onderzoek kan bepaald worden welke factor dit is of welke factoren dit zijn. Deze strategie wordt ook benoemd in het onderzoek van Xie en Peng (2009). In recente studies van onder andere Metlay (2013), Terwel, Harinck, Ellemers, en Daamen (2009) en Connelly, Crook, Combs, Ketchen Jr, en Aguinis (2018) worden competence based trust en integrity based trust samen onderzocht en wordt benevolence based trust achterwege gelaten.
In navolging van de hiervoor genoemde onderzoeken, zal voor dit onderzoek ook alleen gekeken worden naar integrity based trust en comptence based trust omdat het onderzoek zich richt op de vertrouwensrelatie tussen de consument en een bedrijf, en niet naar de relatie van individuen onderling. Connelly et al. (2018) maken in hun onderzoek dezelfde keuze om dezelfde reden.

2.3.2 Concepten die propensity vormen

Naast de hiervoor genoemde drie factoren van vertrouwen, wordt er door Mayer et al. (1995) nog gesproken over propensity. Er zijn een drietal concepten die gerelateerd zijn aan propensity die van belang zijn voor dit onderzoek. Deze worden hieronder toegelicht.

Initial trust

In de context van dit onderzoek is initial trust het vertrouwen in een nog onbekende online winkel waarmee de consument nog niet eerder zaken heeft gedaan (McKnight, Choudhury, & Kacmar, 2002b). Bigley en Pearce (1998) beschrijven in hun artikel het belang van initial trust als volgt. Onbekende actoren zijn actoren die nog geen betekenisvolle informatie over elkaar hebben. Door het hebben van onderlinge interactie, krijgen actoren deze betekenisvolle informatie over elkaar. In de context van e-commerce is het doen van bijvoorbeeld een aankoop een vorm van onderlinge interactie. Na deze interactie heeft de klant de mogelijkheid om te toetsen of zijn/haar initiële vertrouwen terecht is geweest of niet. De resultaten van dergelijke handelingen zijn van invloed op het beeld wat iemand vormt over een bedrijf en dus ook op het vertrouwensbeeld wat de consument over dat bedrijf vormt (McKnight et al., 2002b). De periode van het bekijken van de website van de verkopende partij en het oriënteren op het bedrijf ligt in het domein van initial trust. Om zo goed mogelijk de invloed van de variabelen in dit onderzoek te kunnen meten is het dus van belang om het onderzoek uit te voeren in het domein van initial trust, bijvoorbeeld door gebruik te maken van fictieve bedrijven. Hiermee wordt voorkomen dat respondenten de vragen beantwoorden op basis van andere (eerdere) ervaringen wat de beantwoording van de vragen zou kunnen beïnvloeden.

Institution based trust

Wanneer iemand op basis van inital trust een aankoop doet, gaat deze kopende partij uit van andere informatie waarop hij/zij vertrouwen baseert dan op basis van eerdere ervaringen bij dat betreffende bedrijf. Vanuit de literatuur wordt beschreven dat de consument in dat geval uitgaat van institution based trust (Bachmann & Inkpen, 2011). Institution based trust is het vertrouwen dat noodzakelijke condities aanwezig zijn die de waarschijnlijkheid vergroten van een succesvol resultaat (Bachmann & Inkpen, 2011). In het geval van e-commerce is dat dus

het vertrouwen in het internet op zich als betrouwbaar instituut voor het doen van aankopen (McKnight, Choudhury, & Kacmar, 2002a). Dit onderzoek vindt plaats in het domein van initial trust. Het is daarom van belang om de mate van institution based trust van de populatie ten opzichte van het internet in kaart te brengen omdat dat van invloed kan zijn bij de beantwoording van de vragen (McKnight et al., 2002a).

Disposition to trust

Disposition to trust gaat nog een stap verder dan institution based trust. Disposition to trust gaat over de mate waarin iemand bereid is om afhankelijk te zijn van anderen over een breed spectrum van situaties. Het gaat bijvoorbeeld over het vertrouwen wat iemand heeft in de mensheid in het algemeen (McKnight et al., 2002a). Wanneer dit concept mee wordt genomen in het onderzoek, zou het onderzoek te omvangrijk worden vanwege de extra hoeveelheid vragen. Daarmee zou de enquête weer langer worden dan hij al is en wordt de kans groter dat respondenten afhaken in de beantwoording van hun vragen. Daarnaast gaat dit concept nog weer dieper in op vertrouwen dan institution based trust en door het meenemen van dit concept in het onderzoek zou de focus te veel verschuiven van het initiële onderzoek naar dieperliggende concepten. Het concept voegt daardoor te weinig toe aan het onderzoek, in afweging met het risico wat een te lange vragenlijst met zich meebrengt. Er is daarom voor gekozen om het concept ter kennisgeving aan te nemen, maar niet verder mee te nemen in dit onderzoek.

2.4 Vertrouwen en privacy

Op basis van de literatuur kan dus gesteld worden dat legitimiteit een gefundeerd concept is om te kunnen verklaren waarom organisaties handelen zoals ze handelen. Hieruit voortkomend blijkt dat legitimiteit een sterke relatie heeft met vertrouwen en dat vertrouwen voor consumenten een belangrijke kernwaarde is om een relatie aan te gaan met een bedrijf. Voor bedrijven is dat interessant, omdat dat hun omzet verhoogt (Aiken & Boush, 2006; Flavián & Guinalíu, 2006). In deze paragraaf wordt ingegaan op de relatie tussen vertrouwen en privacy, omdat privacy uiteindelijk de context is waarbinnen vertrouwen bekeken wordt.

Organisaties willen meer de nadruk leggen op het opbouwen van langdurige relaties met de klant, waardoor vertrouwen ook een steeds belangrijkere rol heeft gekregen (Doney & Cannon, 1997; Garbarino & Johnson, 1999). Een succesvolle relatie vergt van bedrijven dat ze transparant zijn in de manier waarop ze omgaan met persoonlijke gegevens van de consument. Consumenten daarentegen moeten bereid zijn om persoonlijke informatie met bedrijven te delen om bedrijven daadwerkelijk de kans te geven om een relatie met de consument aan te gaan; bijvoorbeeld via het versturen van gepersonaliseerde direct mail (Milne & Boza, 1999). Hieruit blijkt dat vertrouwen en privacy nauw met elkaar verbonden zijn. Dat blijkt ook uit het onderzoek van Flavián en Guinalíu (2006), uitgevoerd in Spanje. Zij hebben onderzoek gedaan naar het effect van privacy op de mate waarin consumenten, vertrouwen hebben in een website. Binnen privacy hebben zij vooral gekeken naar het gevoel van veiligheid bij consumenten. Ook hebben ze onderzoek gedaan naar de relatie tussen vertrouwen en de loyaliteit die consumenten hebben naar een bedrijf toe. Uit het onderzoek blijkt dat de loyaliteit van een individu naar een bedrijf toe, samenhangt met de mate van vertrouwen. Ook blijkt uit het onderzoek dat vertrouwen van consumenten in een website,

wordt beïnvloed door privacy en dan met name hoe organisaties omgaan met de persoonsgegevens van consumenten.

2.4.1 Privacy policy

De relatie tussen vertrouwen en privacy is verder onderzocht door Wu et al. (2012). Zij hebben onderzoek gedaan onder studenten in Rusland en Taiwan, en hebben aangetoond dat er een verband is tussen de inhoud van een privacy policy en de mate van vertrouwen. In het onderzoek hebben ze specifiek gekeken naar de elementen ***Notice***, ***Choice***, ***Access***, ***Security*** en ***Enforcement*** van de privacy policy. Hiertoe kwamen zij omdat Liu et al. (2005) eerder een model hebben ontwikkeld waarin ze de relatie aantonen tussen de privacy perceptie van een individu en de intentie tot het doen van een aankoop. Uit hun onderzoek blijkt namelijk dat een succesvolle relatie tussen koper en verkoper, afhankelijk is van de mate van vertrouwen wat de koper heeft in de verkoper en dat privacy van grote invloed is op vertrouwen. Dit onderzoek toonde echter niet aan uit welke elementen een privacy policy moet bestaan of aan welk format het moet voldoen maar alleen dat er een relatie is. Wu et al. (2012) hebben met hun onderzoek wel aangetoond aan welke elementen een privacy policy moet voldoen in relatie tot vertrouwen. Wat ze echter wel in hun onderzoek vermelden, is dat het per cultuur kan verschillen wat de invloed van deze elementen op het vertrouwen van consumenten is. Dat maakt dat het interessant is om dit onderzoek gedeeltelijk te herhalen in Nederland.

2.4.2 Trustmark

Naast het hebben van een gedegen en zichtbaar privacy policy, wordt er in het onderzoek van Liu et al. (2005) ook geschreven over de invloed van een 'trustmark', een keurmerk, op het vertrouwen van consumenten in organisaties. Een trustmark wordt gedefinieerd als "*any third-party mark, logo, picture, or symbol that is presented in an effort to dispel consumers' concerns about Internet security and privacy and, therefore, to increase firm specific trust levels."* (Aiken, Osland, Liu, & Mackoy, 2003). Echter wordt dit niet als aparte variabele gemeten in het onderzoek, maar gezien als onderdeel van een andere variabele, namelijk vertrouwen. Het is dus niet duidelijk of het hebben van een 'trustmark' op zich van invloed is op het vertrouwen van consumenten. Dit is wel onderzocht in een later onderzoek door Aiken en Boush (2006). Zij hebben gekeken naar een trustmark, advertenties en reviews in relatie tot vertrouwen bij studenten in Amerika. Daar kwam uit dat het hebben van een trustmark de grootste invloed heeft van de drie onderzochte variabelen op het vertrouwen van consumenten. Ook Thompson, Tuzovic, en Braun (2019) concluderen in hun onderzoek dat het gebruik van een trustmark het online vertrouwen van consumenten verhoogt, de aankoop bereidheid vergroot en de risicoperceptie verlaagt. In Nederland is er op dit moment nog geen officieel AVG-keurmerk beschikbaar. Op de website van de Autoriteit Persoonsgegevens is te lezen dat op dit moment in Nederland nog geen certificatie-instellingen zijn geaccrediteerd voor het afgeven van AVG-certificaten, maar dat ze er wel aan werken om dat op termijn te realiseren (Autoriteit Persoonsgegevens, 2019a) . Alle bedrijven die op dit moment claimen een AVG-keurmerk af te kunnen geven en daarin samenwerken met de Autoriteit Persoonsgegevens, zouden volgens de organisaties onjuiste informatie verspreiden. Wat Wu et al. (2012) in hun onderzoek benoemden en wat ook blijkt uit het onderzoek van Park, Gunn, en Han (2012) is dat culturele verschillen wel degelijk invloed hebben in de manier waarop consumenten aankijken tegen vertrouwen in relatie tot e-

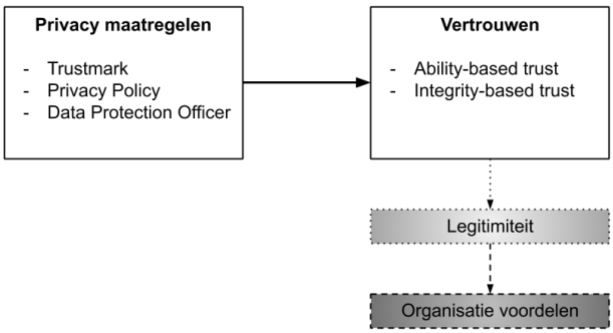
commerce. Daarom is het interessant om ook dit onderzoek gedeeltelijk te herhalen in Nederland.

2.4.3 Data protection officer

Organisaties zijn in bepaalde situaties verplicht een data protection officer (DPO) (ook wel functionaris gegevensbescherming (FG) genoemd) aan te stellen. Dit is iemand die binnen de organisatie toezicht houdt op de toepassing en naleving van de AVG (Autoriteit Persoonsgegevens, 2019b). Hiervoor heeft de Autoriteit Persoonsgegevens een richtlijn opgesteld, waarin bijvoorbeeld beschreven staat aan wat voor profiel iemand moet voldoen en wat zijn/haar taken zijn. Voor zover bekend is er nog geen onderzoek gedaan wat de relatie is van de aanwezigheid van een FG of DPO binnen een organisatie op het vertrouwen van consumenten. In een recent onderzoek van Recio (2017) wordt deze relatie echter wel verondersteld, aangezien de DPO bijdraagt aan de accountability van een organisatie en accountability zou leiden tot vertrouwen, maar dat hebben zij niet wetenschappelijk onderzocht.

2.5 Conceptueel model

Het conceptueel model is een visuele weergave van de verwachte oorzaak-gevolgrelatie in een onderzoek (Scribber, 2014). Zoals blijkt uit figuur 1 wordt er een relatie verondersteld tussen verschillende privacy maatregelen die organisaties kunnen toepassen en het vertrouwen wat consumenten hebben in de organisatie. In paragraaf 2.2 is reeds besproken dat vertrouwen leidt tot legitimiteit en dat legitimiteit verschillende voordelen heeft voor een organisatie. Deze voordelen zijn dat de organisatie als waardevoller, betekenisvoller, voorspelbaarder en betrouwbaarder wordt gezien. De concepten legitimiteit en organisatie voordelen zijn verder geen onderdeel van dit onderzoek. In dit onderzoek wordt alleen gekeken naar de relatie tussen privacy maatregelen en vertrouwen.

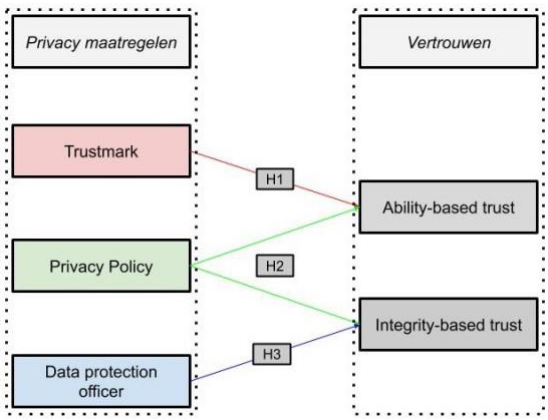


Figuur 1: conceptueel model

2.6 Hypotheses

Op basis van het literatuuronderzoek en het conceptueel model, kunnen er een aantal hypotheses geformuleerd worden voor het onderzoek. Deze zijn schematisch weergegeven in figuur 2 en betreffen de volgende hypotheses:

Hypothese 1: Trustmarks
Een zichtbare trustmark heeft een positieve invloed op het vertrouwen van Nederlandse consumenten in e-commerce bedrijven.



Figuur 2: schematische weergave variabelen

Hypothese 2: Inhoudelijke privacy policy
Een inhoudelijk goede privacy policy heeft een positieve invloed op het vertrouwen van Nederlandse consumenten in e-commerce bedrijven.

Hypothese 3: Data Protection Officer
Het hebben van een DPO heeft een positieve invloed op het vertrouwen van Nederlandse consumenten in e-commerce bedrijven.

De resultaten van deze drie hypotheses vormen samen het antwoord op de hoofdvraag van dit onderzoek. Door aan iedere afhankelijke variabele, onafhankelijke variabelen te koppelen worden de verschillende vormen van vertrouwen gemeten. Privacy policy wordt gekoppeld aan beide vormen van vertrouwen, omdat je zou kunnen stellen dat het zowel iets over ability-based trust als over integrity-based trust zegt.

3. Methodologie
Uit hoofdstuk 2 zijn een aantal belangrijke punten naar voren gekomen die de basis vormen voor dit hoofdstuk. In dit hoofdstuk worden deze punten besproken, indien nodig verder toegelicht en wordt besproken hoe het onderzoek uitgevoerd wordt.

3.1 Unit of analysis
De unit of analysis is voor dit onderzoek de Nederlandse consument. Er zijn variabelen op organisatieniveau en op individueel niveau. Maar aangezien het onderzoek zich specifiek richt op het vertrouwen van consumenten in relatie tot keuzes die organisaties kunnen maken om dat vertrouwen mogelijk te beïnvloeden, is de unit of analysis de consument en niet de organisatie. Uit de literatuur in hoofdstuk 2 blijkt dat er gerelateerde onderzoeken bestaan, maar dat deze verschillende onderzoeken alleen hebben plaatsgevonden onder Amerikaanse, Spaanse, Russische of Taiwanese inwoners. Bepaalde delen van deze onderzoeken kunnen daarom gereproduceerd worden bij Nederlandse consumenten om te bekijken of de conclusies die zij trekken ook gelden voor deze populatie. Zoals in paragraaf 2.4.1 en paragraaf 2.4.2 al reeds is besproken, zijn culture verschillen namelijk mogelijk van invloed op de vertrouwensperceptie van consumenten in e-commerce organisaties. Een ander argument om te kijken naar de Nederlandse consument, is dat het onderzoek wordt uitgevoerd in de context van de AVG, welke alleen in Nederland van kracht is. Tenslotte zal het onderzoek zich richten op personen vanaf 18 jaar die wel eens aankopen doet. Vanaf 18 jaar wordt iemand als volwassen gezien en mag dan volgens artikel 488 van het burgerlijk wetboek, officieel zelf beslissingen nemen. Dit houdt ook in dat iemand dan dus zonder toestemming van de ouders iets (online) mag aanschaffen.

3.2 Keuze onderzoeksmethode
Saunders, Lewis, en Thornhill (2016, p. 165) schrijven in hun boek dat er allereerst een keuze gemaakt dient te worden wat voor soort onderzoek er plaats zal vinden; kwalitatief, kwantitatief of een mix van beide. Kwantitatieve onderzoeksmethoden worden vaak gebruikt om relaties tussen variabelen aan te tonen en om bestaande theorieën te testen. Kwalitatieve onderzoeksmethoden worden vaak gebruikt om meningen van participanten te krijgen en een verband tussen deze meningen te ontdekken. Kwalitatief onderzoek wordt vaak gebruikt

bij het ontwikkelen van nieuwe theorieën. Dit onderzoek zal zich in de basis richten op het aantonen van relaties tussen variabelen, zoals blijkt uit figuur 1, en daarom kwantitatief van aard zijn. Anderzijds zijn bepaalde onderdelen van de studie meer kwalitatief van aard, omdat hier nog niet eerder onderzoek naar gedaan is. Dit geldt voor het combineren van deze specifieke set variabelen en de relatie tussen een DPO en vertrouwen op zich. Volgens Saunders et al. (2016, p. 174) zijn er vier vormen van onderzoek te onderscheiden: exploratief, descriptief, verklarend en evaluerend. Dit onderzoek is deels exploratief van aard, aangezien er nog niet eerder onderzocht is wat een DPO voor effect heeft op het vertrouwen van consumenten in onlineorganisaties. Maar ook deels evaluerend van aard aangezien een eerder aangetoonde relatie tussen een keurmerk, een privacy policy en vertrouwen, weliswaar in een andere context, ook wordt getoetst.

3.2.1 Onderzoeksvorm

Saunders et al. (2016, p. 178) beschrijven in hun boek een aantal vormen van onderzoek, bijvoorbeeld een experiment, enquête en case study. De vorm die voor dit onderzoek is gekozen, is enquête en experiment. Een enquête wordt vaak gebruikt voor exploratief onderzoek. Bovendien bieden ze de onderzoeker de mogelijkheid om kwantitatieve data te standaardiseren en goed met elkaar te vergelijken met behulp van statistiek. Tenslotte geeft het vaak antwoord op de wat, wie, waar en hoeveel vragen (Saunders et al., 2016, p. 181). Voor dit onderzoek wordt een brede groep personen benaderd. Daarnaast worden in de enquêtes verschillende vormen en situaties voorgelegd aan de respondent. Dit maakt dat het onderzoek ook een experimenteel karakter heeft.

3.2.2 Variabelen

Om te kunnen bepalen welke onderzoeksstrategie gehanteerd gaat worden, is het belangrijk om de verschillende variabelen in kaart te brengen die van belang zijn tijdens dit onderzoek. In tabel 1 zijn de variabelen schematisch weergegeven.

Tabel 1: overzicht variabelen

Variabele	**Soort variabele**	**Omschrijving**	**Relatie met**
Privacy Policy	Onafhankelijke variabele	Dat er een relatie is tussen privacy policy en vertrouwen is in eerdere onderzoeken aangetoond, maar niet eerder in de context van de AVG en dus niet in Nederland.	Ability-based trust & integrity based trust
Trustmarks	Onafhankelijke variabele	Dat er een relatie is tussen trustmark en vertrouwen is in eerdere onderzoeken aangetoond, maar niet eerder in de context van de AVG niet dus in Nederland.	Integrity-based trust
Data Protection Officer (DPO)	Onafhankelijke variabele	Dat er een relatie is tussen een data protection officer en vertrouwen wordt in de literatuur gesuggereerd, maar is nog niet eerder aangetoond of onderzocht in de context van de AVG.	Ability-based trust
Ability-based trust	Afhankelijke variabele	Verondersteld wordt dat een enkele of meerdere variabelen invloed hebben op ability-based trust.	Privacy policy & DPO
Integrity-based trust	Afhankelijke variabele	Verondersteld wordt dat een enkele of meerdere variabelen invloed hebben op integrity-based trust.	Privacy policy & Trustmarks

3.3 Onderzoeksopzet

In deze paragraaf wordt de onderzoeksopzet besproken. De opzet is onderverdeeld in de drie verschillende fases van onderzoek en geeft per fase op hoofdlijnen weer hoe het onderzoek is uitgevoerd.

3.3.1 Fase 1: voorbereiding

Het experiment is uitgevoerd middels een enquête. Iedere respondent kreeg willekeurig één van de acht scenario's aangeboden waarin van iedere verklarende variabele één variant is opgenomen. Een scenario bevat bijvoorbeeld wel een trustmark, een goede privacy officer, maar een slechte privacy policy. Een respondent kreeg dus nooit beide varianten van een verklarende variabele te zien, maar altijd één variant. In totaal zijn er 2 (varianten) x 3 (variabelen) dus 2x2x2=8 verschillende soorten scenario's mogelijk. Iedere respondent kreeg vervolgens een aantal vragen over vertrouwen. Deze vragen waren voor iedere respondent gelijk. In deze fase is ook de enquête vormgegeven. Bij het vormgeven van de scenario's is gebruikgemaakt van de inzichten van bestaande onderzoeken. Deze onderzoeken zijn wetenschappelijk gefundeerd en hebben reeds plaatsgevonden wat de betrouwbaarheid en validiteit verhoogt. Specifiek gaat het hierbij om de onderzoeken van Aiken en Boush (2006) en Wu et al. (2012). In tabel 2 is schematisch weergegeven hoe beide onderzoeken zijn uitgevoerd. In bijlage 3 is precies weergegeven welke vragen uit welke onderzoeken zijn gebruikt.

Tabel 2: schematische weergave van bestaande onderzoeken

	Het onderzoek van Aiken & Boush	**Het onderzoek van Wu et al.**
Onderzoeksvorm	Enquête & experiment	Enquête
Verdieping van onderzoeksvorm	26 vragen op een 9-punt Likert schaal. Tevens zijn de onafhankelijke variabelen ook gecombineerd getoetst.	Er zijn verschillende stellingen voorgelegd met antwoordmogelijkheden op een 5-punt Likert schaal.
Populatie	Mailinglist van een radiostation van een grote universiteit in de USA	Online respondenten van 18 jaar en ouder in Rusland en Taiwan.
Aantal respondenten	299	500
Gebruikte statistische methoden	Pearson correlatie coëfficiënten, Cronbach's alpha, eigenvalue, RMSEA en CFI (Factor Matrix).	Cronbach's alpha, factor analyse, PCA, SEM, CFI, RMSEA, IFI, X2,

Met name de onderzoeksopzet van Aiken en Boush (2006) komt overeen met de intentie van dit onderzoek en is om die reden geraadpleegd. Het onderzoek van Wu et al. (2012) is vooral gebruikt voor de input voor de scenario's. Tenslotte is er in de vormgeving van de scenario's gebruikgemaakt van een fictief bedrijf om aan te sluiten bij het concept van initial trust, zoals beschreven in paragraaf 2.3.2. Voor een volledige beschrijving van de vormgeving van de enquête, zie bijlage 3. In paragraaf 3.4 wordt verder ingegaan op de genomen maatregelen ten behoeve de betrouwbaarheid en validiteit van het onderzoek.

3.3.2 Fase 2: afnemen van het experiment

Voorafgaand aan het werkelijke onderzoek, is in een pilot groepje van vier proefpersonen de enquête getest. Eventuele (technische) fouten en onduidelijkheden zijn hierdoor in een vroeg stadium ontdekt. Zo is er gecontroleerd of deze testpersonen de vragen begrijpen, op de juiste manier interpreteren, de vragenlijst goed kunnen invullen en worden onduidelijkheden

in kaart gebracht. De vier proefpersonen hebben allen de enquête afzonderlijk ingevuld zodat ongestuurd duidelijk werd waar de mogelijke verbeterpunten liggen. De proefpersonen zijn allemaal bekenden van de onderzoeker waardoor verwacht wordt dat de mate van feedback volledig is en de kwaliteit goed. De proefpersonen wisselen van opleidingsachtergrond en leeftijd om ook hier de diversiteit terug te laten komen die in het definitieve onderzoek terug zal komen. Elke vorm van feedback is serieus bekeken en er is kritisch gekeken of de enquête aangepast diende te worden. In bijlage 3 is precies beschreven welke feedback de proefpersonen hadden en wat er met deze feedback is gedaan. De resultaten van de testgroep zijn niet meegenomen in de resultaten van het onderzoek.

In de periode 01 april tot en met 08 mei 2020 zijn de definitieve enquêtes ingevuld door de respondenten. Het uiteindelijke doel is om van tenminste 60 respondenten informatie te verzamelen. Om het aantal respondenten te kunnen bepalen, is gebruikgemaakt van het artikel van VanVoorhis en Morgan (2007). In tabel 3 van het artikel schrijven ze dat voor het meten van verschillen per groep, er optimaal 30 respondenten per groep nodig zijn, maar nooit minder dan zeven respondenten. Een groep is in dit geval één variant van een van de variabelen. Echter worden de variabelen in dit onderzoek nooit losstaand getoetst, maar altijd in combinatie met elkaar. Dat betekent dat in ieder scenario altijd van alle drie de variabelen, één variant voorkomt. Zoals in paragraaf 3.3.1 is uitgelegd, zijn er acht scenario's te onderscheiden. In deze acht scenario's komt iedere variant van de variabele, vier keer voor.

Om vervolgens te kunnen berekenen hoeveel respondenten er in totaal nodig zijn, is het optimale aantal respondenten (dat zijn er 30), gedeeld door het aantal keer dat een variabele voorkomt in de scenario's (dat is vier keer) en is dat vermenigvuldigd met het aantal scenario's (dat zijn er acht). Optimaal gezien zijn er dus 60 respondenten nodig die de enquête volledig invullen. Minimaal zouden er dus 7/4 = +/- 2 * 8 = 16 respondenten nodig zijn. Voor een volledige onderbouwing van het aantal benodigde respondenten zie bijlage 2. Het voordeel van het combineren van verschillende variabelen in één scenario, is dat er minder respondenten nodig zijn. Daarnaast kan hierdoor goed in kaart worden gebracht wat de invloed is van een bepaalde variabele op vertrouwen, wordt de invloed van combinaties van variabelen gemeten waardoor in theorie vertrouwen als geheel wordt gemeten en niet enkel de twee losstaande concepten ability-based trust en integrity-based trust. Een nadeel is dat de vragenlijst complex kan worden en langer is dan wanneer ieder concept los zou worden gemeten. De proef respondenten gaven echter aan dat de lengte van de vragenlijst precies goed was. Hierin worden dus geen problemen voorzien. In het uiteindelijke aantal is dat terug te zien. In totaal hebben namelijk 81 respondenten de enquêtes ingevuld. In hoofdstuk 4 worden de resultaten verder besproken.

De enquêtes zijn verspreid in de kennissenkring van de onderzoeker. Saunders et al. (2016, p. 713) omschrijft dit als 'convenience sampling' als onderdeel van een brede methode genaamd 'haphazard sampling'. Hiervan is sprake als de respondenten worden geselecteerd omdat ze nu eenmaal makkelijk te benaderen zijn. Dit is een vorm van non-probability sampling waarbij de kans of waarschijnlijkheid dat een sample (respondent in dit geval) gekozen wordt, niet bekend is. Ondanks dat het een veelvoorkomende vorm van sampling is, is het gevoelig voor bias en voor factoren die vaak niet te beïnvloeden zijn (Saunders et al., 2016, p. 304). Echter wordt er wel de kanttekening geplaatst dat er ook gekeken dient te worden naar de context van het onderzoek, alvorens 'convenience sampling' wordt geclassificeerd als minder

geloofwaardige methode. Voor dit onderzoek is 'convenience sampling' een minder groot probleem om twee redenen. Allereerst is het argument dat wordt aangedragen door Saunders ook van toepassing, namelijk dat alles beter is dan geen sample waardoor er überhaupt geen onderzoek kan plaatsvinden. Zolang er maar enige variatie in de populatie zit die vergelijkbaar is met de variatie van de te onderzoeken populatie hoeft het zelfs geen probleem te zijn. En dat is het tweede argument wat de keuze voor deze methode rechtvaardigt. Dit onderzoek richt zich op de Nederlandse consument in het algemeen, wat een zeer ruime populatie is. Zolang deze variatie terug te vinden is in de respondenten van de enquête, zal dat voor de conclusies standhouden. Tijdens het afnemen van de enquête wordt daarom van iedere respondent gevraagd om de volgende profielkenmerken te delen: leeftijdscategorie; geslacht; de mate van ervaring met het doen van online aankopen. De hierboven genoemde onderzoeken hebben bovendien ook dergelijke achtergrondgegevens van respondenten gevraagd om deze redenen. Ook worden nog wat aanvullende vragen gesteld die aansluiten bij het overkoepelende concept propensity. Niet om propensity als concept te meten, maar wel omdat het mogelijk de antwoorden van de respondenten kan beïnvloeden en daarmee dus ook de uitkomsten van het onderzoek. Deze vragen worden dus meegenomen om de betrouwbaarheid van het onderzoek te vergroten.

3.3.3 Fase 3: analyse

Nadat de enquêtes zijn afgerond worden de resultaten geïnterpreteerd via verschillende testen. Om te toetsen of de enquêtes kwalitatief goed in elkaar zitten, wordt voor dit onderzoek bijvoorbeeld gebruikgemaakt van de factoranalyse en Cronbach's Alpha. Deze methode wordt ook door de hierboven genoemde onderzoeken gebruikt. Verder wordt er gebruikgemaakt van de T-test, ANOVA, Mann-Whitney u test, Kolmogorov-Smirnov en de Shapiro Wilk en tenslotte de Levene's test. In hoofdstuk 4 wordt besproken waarom ze zijn gebruikt en wat ze precies testen.

3.4 Validiteit en betrouwbaarheid

In deze laatste paragraaf worden de validiteit en betrouwbaarheid van het onderzoek besproken. De verschillende vormen worden besproken en vervolgens wordt er aangegeven welke concrete maatregelen er zijn genomen om te zorgen voor een zo valide en betrouwbaar mogelijk onderzoek. De betrouwbaarheid van het onderzoek houdt in dat het onderzoek te repliceren is en consistent is. Validiteit betekent in het algemeen dat de onderzoeksresultaten kloppen met de werkelijkheid en dat het onderzoek generaliseerbaar is. Binnen validiteit kan je spreken van interne validiteit en externe validiteit. Interne validiteit gaat vooral over de consistentie van het onderzoeksproject, terwijl externe validiteit meer gaat over generaliseerbaarheid gaat. Daarnaast is er een derde vorm van validiteit namelijk meet validiteit wat ingaat op het gebruikte onderzoeksinstrument. Tenslotte wordt er nog gesproken over constructvaliditeit wat inhoudt of de begrippen en variabelen goed zijn bepaald (Saunders et al., 2016, p. 202). In tabel 3 is schematisch weergegeven welke maatregelen er zijn genomen om de validiteit en betrouwbaarheid van het onderzoek te waarborgen.

Tabel 3: genomen maatregelen betrouwbaarheid en validiteit

	GENOMEN MAATREGEL	TOELICHTING
INTERNE VALIDITEIT	Het onderzoek is afgebakend en niet te groot.	Binnen vertrouwen wordt er gebruikgemaakt van twee variabelen en binnen privacy maatregelen van drie variabelen.
	De onderzoeksmethoden zijn geschikt als meetinstrument.	Een experiment in combinatie met het uitzetten van een enquête is in een eerder, vergelijkbaar, onderzoek uitgevoerd. Dit is dus een reeds beproefde methode.
	De enquête wordt vooraf getest.	De enquête wordt getest op proefpersonen die ook behoren tot de onderzoekspopulatie.
	Voorkomen van sociaal-wenselijke antwoorden.	De enquêtes worden anoniem afgenomen en vanwege het digitale karakter kan de respondent het onderzoek afnemen zonder dat de onderzoeker de respondent kan beïnvloeden.
	Zo veel als mogelijk gebruikmaken van reeds bestaande vragenlijsten.	Voor zoveel als mogelijk wordt gebruikgemaakt van reeds bestaande vragenlijsten die gebruikt zijn in andere onderzoeken. Deze vragenlijsten zijn vaak al statistisch getoetst wat de validiteit van dit onderzoek ook ten goede komt.
	Gebruikmaken van een fictief bedrijf in de casussen.	Indien er gebruik wordt gemaakt van bestaande bedrijven in de vragenlijst, kan dit invloed hebben in de manier waarop respondenten hun antwoord geven. De respondenten kan namelijk te maken hebben gehad met het bedrijf wat zijn/haar perceptie van vertrouwen heeft beïnvloed ten opzichte van het bedrijf. Om de drie variabalen zo puur mogelijk te meten is het van belang om in het domein van initial trust te blijven (zie ook paragraaf 2.3.2).
	Toetsen van de houding van de respondent t.o.v. e-commerce	Door in de vragenlijst iemand te vragen naar zijn/haar houding ten opzichte van het doen van aankopen online, wordt getoetst of iemand niet vooraf al weerstand heeft tegen het doen van aankopen online. Deze weerstand kan namelijk van invloed zijn op de beantwoording van de vragen.
BETROUWBAARHEID	Verschillende stappen van de analyse zijn transparant.	Er wordt helder omschreven hoe het data-analyse proces heeft plaatsgevonden. Deze omschrijving wordt waar nodig ondersteund met screenshots van de analyses.
	Archiveren van data.	De brondata wordt apart bewaard zodat deze data onaangetast blijft. Bovendien blijft deze data 10 jaar na het uitvoeren van het onderzoek bewaard.
	Kritische peer review	Dit onderzoek staat onder supervisie van een docent van de universiteit. Deze zal het proces kritisch monitoren.
	Voldoende respondenten	Er wordt een minimum van 60 respondenten gehanteerd voor het uitvoeren van het onderzoek, om gedegen uitspraken te kunnen doen over de data. Echter zal het streven zijn om meer respondenten te ondervragen.
CONSTRUCTVALIDITEIT	Begrippen definiëren	Begrippen zijn in het theoretisch kader zo veel als mogelijk gedefinieerd volgens wetenschappelijke bronnen.

	Aan respondenten definities uitleggen	In de enquête zullen, indien nodig, begrippen gedefinieerd worden zodat hier bij het invullen geen misvatting over kan ontstaan bij respondenten.
	Gebruikmaken van reeds bestaande onderzoeken	In reeds bestaande onderzoeken zijn begrippen al geoperationaliseerd en wetenschappelijk onderbouwd. Deze input zal zo veel als mogelijk ook gebruikt worden in dit onderzoek.

4. Onderzoeksresultaten

In dit hoofdstuk worden de resultaten besproken die uit het onderzoek naar voren zijn gekomen. In bijlage 4 is een overzicht te vinden van alle tabellen die relevant zijn ter verdieping op de analyses die zijn gedaan.

4.1 Betrouwbaarheid beantwoording respondenten

Voordat er analyses gedaan kunnen worden is het belangrijk om de betrouwbaarheid van de antwoorden te analyseren. Mocht blijken dat er twijfels bestaan over de betrouwbaarheid van bepaalde respondenten dan dienen deze er eerst uit te worden gefilterd. Hiervoor wordt eerst stilgestaan bij controlepunt 1. Vervolgens moet bekeken worden of er sprake is van een negatieve houding ten opzichte van het doen van online aankopen, zoals is besproken in paragraaf 2.3. Bij controlepunt 2 wordt hierbij stilgestaan.

Controlepunt 1: Aanklikken van dezelfde waardes

Om de uitkomst van dit controlepunt te kunnen bepalen is er een tabel gegenereerd met de totaalscores per respondent op de vragen 1 tot en met 8. Per vraag waren er 6 keuzemogelijkheden. Wanneer een respondent op deze vragen overal hetzelfde antwoord heeft ingevuld komt een respondent op die vragen uit op een totaalscore van 8x1= 8, 8x2=16, 8x3=24, en verder tot 8x6=48. Bij de vragenlijsten waarbij zo'n waarde gevonden is, is handmatig een check gedaan of hier inderdaad allemaal dezelfde waardes zijn ingevuld. Er zijn vier vragenlijsten gevonden waarbij een respondent bij vraag 1 tot en met 8 allemaal dezelfde waarde heeft aangevinkt (respondent 45, 71, 72 en 73). Vervolgens is bij deze respondenten gekeken of er variatie zat in de vragen 9 tot en met 12. Bij drie van de vier respondenten zat er wel variatie in de vragen 9 tot en met 12 waardoor er aangenomen wordt dat deze respondenten de vragen 1 tot en met 8 bewust zo hebben ingevuld. Bij een respondent was er in de vragen 9 tot en met 12 ook geen variatie te vinden. Dat zou erop kunnen duiden dat deze respondent structureel hetzelfde antwoord heeft aangekruist. Het kan echter ook nog steeds daadwerkelijk de mening zijn van deze respondent. Omdat uiteindelijk de betrouwbaarheid van de dataset bovenaan staat, is ervoor gekozen om de antwoorden van deze respondent niet mee te nemen in het onderzoek. De antwoorden van 80 respondenten gaan mee in de analyse van het volgende controlepunt.

Controlepunt 2: Institution based trust

Zoals beschreven in paragraaf 2.3 is propensity een belangrijk concept om mee te nemen in het onderzoek. Controlepunt 2 richt zicht specifiek op institution based trust waarover wordt

gesproken in paragraaf 2.3.2. In tabel 4 is het aantal respondenten per categorie per stelling weergegeven met daarbij het gemiddelde en de standaarddeviatie.

Tabel 4: overzicht score propensity

		HELEMAAL MEE ONEENS	MEE ONEENS	EEN BEETJE MEE ONEENS	EEN BEETJE MEE EENS	MEE EENS	HELEMAAL MEE EENS	GEMIDDELDE	ST. DEVIATIE
1)	**IN DE MEESTE GEVALLEN KOMEN ONLINE VERKOPERS HUN AFSPRAKEN NA**	1	1	1	7	56	15	4,99	0,798
2)	**OVER HET ALGEMEEN HEB IK POSITIEVE ERVARINGEN MET HET DOEN VAN ONLINE AANKOPEN**	0	1	0	5	53	22	4,59	0,905
3)	**IK VOEL MIJ COMFORTABEL BIJ HET DOEN VAN AANKOPEN OP HET INTERNET**	0	2	8	23	35	13	4,60	0,958
4)	**OVER HET ALGEMEEN HEB IK ER VERTROUWEN IN DAT HET KOPEN VAN PRODUCTEN GOED GAAT ALS IK ZE AANSCHAF VIA INTERNET.**	0	2	8	20	42	9	5,17	0,648

Wanneer de theorie uit paragraaf 2.3.2 gevolgd zou worden dan betekent dat, dat de antwoorden van de respondenten die slecht scoren op ‘initial trust’ niet meegenomen moeten worden in de analyses. Om te testen of dit inderdaad significant is, is er een correlatietest uitgevoerd tussen ‘vertrouwen’ en ‘initial trust’. Ook de uitkomst van de factoranalyse is hierin belangrijk, want daaruit blijkt namelijk dat de vragen die gaan over initial trust, ook daadwerkelijk als een component gezien kunnen worden. De factoranalyse wordt in paragraaf 4.3 besproken. Uit de correlatie test komt een waarde van 0,323. Dat betekent dat er sprake is van een zwakke correlatie. Een significantie van 0,004 geeft aan dat deze relatie als significant kan worden gezien. In tabel 5 is dit schematisch weergegeven. Ondanks dat de correlatie zwak is, is er toch voor gekozen om de antwoorden van de

respondenten die het eventueel betreft, te verwijderen. De correlatie is namelijk, ook al is het zwak, wel aanwezig.

Tabel 5: correlatie tussen vertrouwen en initial trust

	CORRELATIE	P-WAARDE	N
INITAL TRUST & VERTROUWEN	0,323	0,004	80

Vervolgens wordt bepaald welke respondenten dit betreft. De maximale totaalscore van een respondent die negatief staat ten opzichte van het doen van online aankopen is 4 x “een beetje mee oneens” of lager. Dus 4x3=12 of lager. Er is 1 respondent die hieraan voldoet. Deze respondent heeft een totaalscore van 8 waaruit blijkt dat deze respondent geen vertrouwen heeft in online webwinkels op zich. Dat betekent dat de antwoorden van deze respondent niet meegenomen worden in de analyses. In totaal worden de antwoorden van 79 respondenten meegenomen in de vervolgonderzoeken.

4.2 Algemene kenmerken populatie

34 respondenten zijn man, 44 respondenten vrouw en 1 anders/wil niet zeggen. Het grootste percentage van de respondenten, namelijk 39,2% valt in de leeftijdscategorie 25-34 jaar. De leeftijdscategorieën 35-44 (15,2%), 45-54 (17,7%) en 55-64 (17,7%) waren daarna het grootst. In de categorieën 18-24 (3,8%) en 65-74 (6,3%) waren de respondenten het minst vertegenwoordigd. Hieruit blijkt dat er sprake is van enige variatie in leeftijd en geslacht van de respondenten maar niet zoveel als bij de feitelijke populatie. Het merendeel, namelijk 72,2% van de respondenten, gaf aan ervaren tot heel erg ervaren te zijn in het doen van online aankopen. Ook gaf het merendeel (74,7%) aan het belangrijk tot heel erg belangrijk te vinden hoe organisaties omgaan met zijn/haar persoonsgegevens. Ondanks dat de onderzochte populatie wat jonger is dan de feitelijke populatie, zit er wel voldoende variatie in om verdere analyses uit te kunnen voeren. De respondenten zijn bovendien ervaren genoeg in het online shoppen om de vragen te kunnen beantwoorden.

4.3 Betrouwbaarheid en validiteit

In deze paragraaf zal stil worden gestaan bij de betrouwbaarheid en validiteit van de vragenlijst. Specifiek worden de factoranalyse en Cronbach’s alpha besproken. Deze twee analyses zijn specifiek van belang wanneer er gebruik is gemaakt van enquêtes. Een factoranalyse bepaalt of de vragen waarvan vooraf is bepaald dat ze gezamenlijk een construct zouden moeten meten, ook daadwerkelijk bij dat construct horen (Field, 2009, p. 786). Met andere woorden, wordt er daadwerkelijk gemeten wat dit onderzoek wil meten? Dit is met name belangrijk voor de vragen waarvan op voorhand wordt verwacht dat ze samen het concept vertrouwen meten en het concept propensity meten, dat ook daadwerkelijk doen. Als de factoranalyse is uitgevoerd, volgt de test waarmee de Cronbach’s alpha wordt gemeten. Cronbach’s alpha zegt iets over de betrouwbaarheid van de vragenlijst door te kijken of verschillende vragen die hetzelfde meten, wat eerder bepaald is met de factoranalyse, op een consistente manier worden beantwoord (Field, 2009, p. 674). Cronbach’s alpha wordt daarom ook wel een betrouwbaarheidsanalyse genoemd. Een hoge score op de Cronbach’s alpha, meestal vanaf 0,800, toont een hoge mate van betrouwbaarheid aan. Wanneer is bepaald welke constructen er gedefinieerd kunnen

worden (via de factoranalyse) en vervolgens blijkt dat ieder construct hoog scoort op de Cronbach's alpha, dan kan geconcludeerd worden dat deze constructen samen een schaal kunnen vormen door de waardes bij elkaar op te tellen. Hiermee kan dan gerekend worden in verdere toetsen. Het is daarom van belang om deze beide testen eerst te doen en in de volgorde zoals is beschreven.

Factoranalyse

Zoals te zien is in tabel 6 scoren vraag 1 tot en met 8 laden hoog op component 1 en de vragen 9 tot en met 12 laden hoog op component 2. Hieruit blijkt dat er twee componenten te onderscheiden zijn, namelijk vertrouwen en institution based trust, zoals ook is verondersteld in hoofdstuk 2. Hieruit blijkt ook dat vragen die volgens de literatuur samen geen construct vormen, ook geen samenhang vertonen. De waarden die in de kolommen staan wordt 'componentlading' genoemd. Als vuistregel wordt vaak gehanteerd dat een variabele goed op een construct laadt als deze een componentlading heeft van meer dan 0,600 (Velicer & Jackson, 1990). Voor alle waardes, waarmee de componenten worden aangetoond, is dit het geval. De factoranalyse laat ook zien dat er geen onderscheid wordt gemaakt tussen ability based trust en integrity based trust en dat deze twee concepten dus gezamenlijk als vertrouwen kunnen worden gezien. Omdat alle vragen zijn gehaald uit reeds bestaande wetenschappelijke onderzoeken, waarin deze vragen ook statistisch getoetst zijn, herbevestigen deze uitkomsten eigenlijk de testen uit deze onderzoeken. Deze herbevestiging was echter wel noodzakelijk om te toetsen of de validatie ook in deze dataset terug te vinden was. Er kan dan ook worden gesproken van een confirmatory factor analysis (Brown, 2015).

Tabel 6: resultaten factoranalyse

Component Matrix[a]

	Component 1	Component 2
5) Deze organisatie gaat goed om met mijn persoonsgegevens	0,902	-0,028
8) De organisatie komt geloofwaardig op mij over	0,888	-0,222
2) De informatie die deze organisatie aanbiedt is eerlijk en transparant	0,868	-0,011
1) De organisatie komt over als een betrouwbare organisatie	0,863	-0,270
7) Deze organisatie is een voorbeeld voor andere organisaties op het gebied van privacy	0,854	-0,131
6) Ook als niemand het zou monitoren zou deze organisatie nog het goede doen	0,820	-0,049
3) Deze organisatie heeft kennis van zaken	0,774	-0,204
4) Als ik bij dit bedrijf iets zou bestellen zou ik er vertrouwen in hebben dat het geleverd wordt	0,667	-0,093
11) In de meeste gevallen komen online verkopers hun afspraken na	0,196	0,703
9) Over het algemeen heb ik er vertrouwen in dat het kopen van producten goed gaat als ik ze aanschaf via internet	0,353	0,690
12) Over het algemeen heb ik positieve ervaringen met het doen van online aankopen	0,243	0,661
10) Ik voel mij comfortabel bij het doen van aankopen op het internet	0,457	0,647

Extraction Method: Principal Component Analysis.

a. 2 components extracted.

Cronbach's alpha

De Cronbach's alpha wordt apart bekeken voor de vragen 1 tot en met 8 en voor de vragen 9 tot en met 12. Hiervoor is gekozen omdat de factoranalyse aantoont dat de vragen 1 tot en met 8 gezamenlijk een construct meten (vertrouwen) en 9 tot en met 12 gezamenlijk een construct meten (institution based trust).

<u>Vertrouwen</u>

De eerste acht vragen scoren een Cronbach's alpha van 0,941. Hiermee scoort de vragenlijst ruim boven 0,800. Het weglaten van bepaalde vragen levert geen tot een zeer minimale verhoging van de Cronbach's alpha waardoor dat niet noodzakelijk is (zie ook bijlage 4). Hiermee kan geconcludeerd worden dat de waardes van de eerste 8 vragen bij elkaar mogen worden opgeteld omdat ze hetzelfde concept meten.

<u>Institution based trust</u>

De vragen 9 tot en met 12 scoren een Cronbach's Alpha van 0,726. Dat is volgens de vuistregel net iets te laag (0,800 of hoger is optimaal) maar is nog altijd boven de 0,700 (wat gezien

wordt als minimale waarde). Het verwijderen van vragen ten behoeve van een hogere Cronbach's Alpha levert bij deze vragen geen resultaat op (zie ook bijlage 4). Hiermee kan ook geconcludeerd worden dat de waardes van vraag 9 tot en met 12 bij elkaar mogen worden opgeteld en omgezet mogen worden tot een schaal, want ze meten hetzelfde concept.

4.4 Gemiddelde scores op vertrouwen

In deze paragraaf zal dieper worden ingegaan op de gegeven antwoorden van de 79 respondenten. Ook worden er verschillende (onderlinge) analyses gedaan tussen de variabelen in de getoonde scenario's en de invloed daarvan op het vertrouwen van de respondenten. In tabel 7 is een overzicht gegeven van de scenario's en de variabelen. Een 'punt' geeft aan dat in dit scenario voor deze variabele de versie is gebruikt die volgens de literatuur het beste zou moeten werken. Scenario 8 heeft geen 'punt' omdat hierin geen enkele goede variant is getoond.

Tabel 7: overzicht varianten per scenario

	KEURMERK	PRIVACY POLICY	DATA PROTECTION OFFICER
1	•	•	•
2	•	•	
3	•		
4		•	
5			•
6		•	•
7	•		•
8			

4.4.1 Gemiddelde totaalscore per scenario

Allereerst wordt er gekeken naar de gemiddelde totaalscore op het concept vertrouwen in relatie tot het getoonde scenario. In tabel 8 is de uitkomst hiervan weergegeven. De scenario's zijn op volgorde van gemiddelde score op vertrouwen gerangschikt. Hoe hoger deze score hoe meer vertrouwen de respondenten hadden, hoe lager deze score hoe minder vertrouwen de respondenten hadden in dat scenario. Hieruit blijkt dat scenario 1 gemiddeld het hoogste heeft gescoord op vertrouwen en de scenario's 5 en 8 het laagste.

Tabel 8: gemiddelde score op vertrouwen

NUMMER SCENARIO	N	GEMIDDELDE	STD. DEVIATIE
1	11	4,5114	1,04501
6	8	4,0938	0,52928
2	7	3,9643	1,03258
4	12	3,6771	0,85190
7	9	3,5278	1,34742
3	9	3,4028	1,27135
5	12	3,1563	0,82249
8	11	3,2045	1,35355
TOTAAL	79	3,6677	1,11335

4.4.2 Gemiddelde totaalscore per variabele

Ook is er gekeken naar de totaalscore per optie van iedere variabele om te kijken of het veranderen van een bepaalde optie van een variabele effect heeft gehad op het vertrouwen van de respondenten in de organisatie. Hierbij zijn de respondenten niet onderverdeeld per

scenario, maar per optie van de variabele die ze hebben gezien. Onderstaand is dit schematisch weergegeven per variabele.

Variabele 1: Keurmerk

Tabel 9: gemiddelde score op vertrouwen keurmerk

OPTIE	GEMIDDELDE SCORE OP VERTROUWEN
1 (EEN KEURMERK AANWEZIG)	3,88
2 (EEN KEURMERK AFWEZIG)	3,49
VERSCHIL	0,39

Variabele 2: Privacy Statement

Tabel 10: gemiddelde score op vertrouwen privacy statement

OPTIE	GEMIDDELDE SCORE OP VERTROUWEN
1 (CORRECT PRIVACY STATEMENT)	4,06
2 (INCORRECT PRIVACY STATEMENT)	3,30
VERSCHIL	0,76

Variabele 3: Data Protection Officer

Tabel 11: gemiddelde score op vertrouwen keurmerk DPO

OPTIE	GEMIDDELDE SCORE OP VERTROUWEN
1 (DPO DIE VOLDOET AAN VOORWAARDEN)	3,80
2 (DPO DIE NIET VOLDOET AAN VOORWAARDEN)	3,53
VERSCHIL	0,27

Uit de uitsplitsing die hierboven is gedaan valt op te maken dat de opties die volgens de literatuur een goede invloed hadden op vertrouwen, hoger scoorden op de vragen over vertrouwen en dat de scenario's waarin de optie aanwezig was die minder goed zou moeten scoren volgens de literatuur in de praktijk ook minder goed blijken te scoren. Opvallend hierin is ook dat de verschillen bij variabele 1 en 3 minder groot zijn dan bij variabele 2 wat zou kunnen duiden op een grotere invloed op vertrouwen dan de overige twee. De tabellen hierboven geven slechts een eerste indruk van de uitkomsten van het onderzoek. Er dienen aanvullende toetsen gedaan te worden om verbanden daadwerkelijk statistisch aan te kunnen tonen. Deze testen worden in de volgende paragraaf gedaan.

4.4.3 Significantie bepalen van de gemiddelde scores

Toetsen significantie binnen scenario's

Allereerst is het belangrijk om te toetsen of de gemiddelde scores op vertrouwen van ieder scenario, en daarmee de verschillen tussen de scores, significant zijn of niet. Hiervoor wordt gebruikgemaakt van de One-Way-ANOVA test (verder genoemd: ANOVA). Deze test wordt gebruikt om te kijken of drie of meer groepsgemiddelden significant van elkaar verschillen. In dit onderzoek worden er acht scenario's onderzocht en daarom is er sprake van meer groepsgemiddelden.

Voordat de ANOVA test wordt uitgevoerd, wordt er eerst gekeken naar de score voor homogeniteit binnen de varianties met behulp van de Levene's test. Op basis van deze test wordt gekeken of je kan concluderen of er aan de voorwaarde is voldaan van gelijke varianties voor de verschillende groepen, een van de voorwaarden van een parametrische test zoals de

ANOVA-test. Deze test is noodzakelijk op het moment dat de aantallen binnen de groepen (sample sizes) wat van elkaar verschillen. Aangezien de scenario's in dit onderzoek niet door evenveel mensen zijn ingevuld, wordt deze test voor de zekerheid uitgevoerd. Wanneer voor deze test de score 0,050 of hoger is, dan is aan de voorwaarde voldaan (Field, 2009, p. 360).

Tabel 12: homogeniteit binnen varianties van scenarios

	LEVENE STATISTIC	SIGNIFICANTIE	DF1	DF2
HOMOGENITEIT BINNEN GEMIDDELDE VERTROUWEN	1,925	0,078	7	71

Uit deze test komt een p-waarde van 0,078, zoals te zien in tabel 12. Dat betekent dat er net aan de voorwaarde is voldaan, maar wel marginaal. Daarom wordt er voor de zekerheid, naast de ANOVA-test, ook de Welch test uitgevoerd om de significatie te bepalen. De Welch test wordt gebruikt in plaats van de ANOVA-test op het moment dat er geen sprake is van homogeniteit. De resultaten zijn af te lezen in tabel 13. Met een p-waarde van 0,061 voor de ANOVA ligt het resultaat iets aan de hoge kant. Voor de Welch test is de p-waarde van 0,052 echter prima. Gezien het experimentele karakter van het onderzoek en gezien de lage aantallen per groep, wordt een p-waarde van tussen 0,052 en 0,061 als voldoende significant beschouwt. Hiermee wordt vastgesteld dat er een significant verschil aanwezig is tussen de verschillende scenario's die zijn toegepast in dit onderzoek.

Tabel 13: Welch-test en ANOVA

	ANOVA				
	Sum of Squares	Df	Mean Square	F	Sig.
BETWEEN GROUPS	16,205	7	2,315	2,042	0,061
WITHIN GROUPS	80,479	71	1,134		
TOTAL	96,684	78			
	WELCH				
	Statistic	Df 1	Df 2	Sig.	
VERTROUWEN GEMIDDELDE TOTAALSCORE	2,327	7	28,799	0,052	

Toetsen significantie binnen variabelen

Nu bepaald is dat de verschillen significant zijn, is het interessant om te kijken waar die verschillen dan precies zitten. Met behulp van de T-toets of de Mann-Whitneytoets wordt gekeken naar de verschillen tussen twee opties van een variabele. In principe wordt de T-toets gebruikt, een parametrische toets, die uitgaat van een tweetal basisprincipes namelijk: een normaalverdeling en homogeniteit van variatie, zoals ook is besproken bij de ANOVA test (Field, 2009, p. 133). Of er sprake is van een normaalverdeling kan worden afgeleid uit de uitkomsten van de Kolmogorov-Smirnov of de Shapiro Wilk toets (Field, 2009, p. 144). Uit de analyse van Yap en Sim (2011) blijkt dat het resultaat van de Shapiro–Wilktest vaak als het betrouwbaarst kan worden gezien dus binnen dit onderzoek zal die worden afgelezen. Wanneer de uitkomst van deze test een p-waarde van 0,05 of hoger heeft dan is er sprake van een normale verdeling. Als er sprake is van een normaalverdeling dan kan de T-toets prima worden gebruikt. Als er sprake is van een niet normaalverdeling dan wordt naast de T-toets, ook de Mann-Whitneytoets uitgevoerd (Field, 2009, p. 344). Wanneer de T-toets wordt uitgevoerd laat de resultatentabel ook automatisch de uitkomst van Levene's Test for Equality zien. De uitkomsten van deze test laat zien of de variantie van beide groepen gelijk is (het

andere basisprincipe). Hiervan is sprake wanneer de p-waarde van deze test 0,05 of hoger is. Onderstaand is per variabele aangegeven of er sprake is van een normaalverdeling of niet en zijn de uitkomsten van de T-toets en, indien nodig, ook van de Mann-Whitneytoets weergegeven.

Variabele 1: Keurmerk

Uit de resultaten van de Shapiro Wilk toets blijkt dat de data voor 'een keurmerk was aanwezig' niet normaal verdeeld is, aangezien deze p-waardes lager dan 0,05 liggen, zie ook tabel 14. Daarom wordt naast de T-toets ook de Mann-Whitneytoets uitgevoerd. De p-waardes voor 'een keurmerk was niet aanwezig' liggen hoger dan 0,05 dus die zijn wel normaal verdeeld.

Tabel 14: verdeling groepen variabele 1

	Shapiro Wilk		
	Statistic	df	Sig.
Een keurmerk was aanwezig	0,931	36	0,027
Een keurmerk was niet aanwezig	0,974	43	0,418

Uit de resultaten van de T-test, zie tabel 15, blijkt dat er sprake is van minimale significantie van 0,118. Echter vanwege het experimentele karakter van dit onderzoek zou dat een acceptabele waarde zijn. Er is bovendien sprake van homogeniteit binnen de varianties want de p-waarde voor de Levene's test is hoger dan 0,05.

Tabel 15: resultaten T-test variabele 1

	Beschrijvend			**T-Test**			**Equal Variances**
	N	Mean	Std.Deviation	*t*-value	df	p-value	Levene's Test
Een keurmerk was aanwezig	36	3,8819	1,22327	1,580	77	0,118	0,282 (Equal variances assumed)
Een keurmerk was niet aanwezig	43	3,4884	,99134				

Uit de Mann-Whitney U test komt een significantere p-waarde van 0,068. Deze is ook boven de gewenste p-waarde van 0,05 maar ligt een stuk lager dan de p-waarde van de T-test. Zie ook tabel 16.

Tabel 16: resultaten Mann-Whitney U test variabele 1

	Vertrouwen
Mann-Whitney U	588,500
Wilcoxon W	1534,500
Z	-1,828
Sig.	0,068

Conclusie

De 36 deelnemers die een keurmerk hebben gezien (M = 3,88, SD = 1,22), vergeleken met de 43 deelnemers die geen keurmerk hebben gezien (M = 3,49, SD = 0,99), scoorden significant beter op vertrouwen U = 588,5, z = -1,828, p = 0,068.

Variabele 2: Privacy statement

Uit de resultaten van de Shapiro Wilk toets blijkt dat de data voor 'het privacy statement was goed' en voor 'het privacy statement was niet goed' beide normaal is verdeeld. Voor beide testen liggen de p-waardes namelijk hoger dan 0,05, zie ook tabel 17. Dat betekent dat alleen de T-toets wordt uitgevoerd.

Tabel 17: verdeling groepen variabele 2

	Shapiro Wilk		
	Statistic	df	Sig.
Het privacy statement was goed	0,969	38	0,373
Het privacy statement was niet goed	0,955	41	0,101

Uit de resultaten van de T-test, zie tabel 18, blijkt dat er sprake is van een significant verschil tussen beide opties. Een p-waarde van 0,002 ligt namelijk onder de algemene gewenste waarde van 0,005. Er is bovendien sprake van homogeniteit binnen de varianties want de p-waarde voor de Levene's test is hoger dan 0,05.

Tabel 18: resultaten T-test variabele 2

	Beschrijvend			T-Test			Equal Variances
	N	Mean	Std.Deviation	*t*-value	df	p-value	Levene's Test
Het privacy statement was goed	38	4,0592	0,92028	3,180	77	0,002	0,085 (Equal variances assumed)
Het privacy statement was niet goed	41	3,3049	1,16326				

Conclusie

De 38 deelnemers die een goed privacy statement hebben gezien (M = 4,06, SD = 0,92), vergeleken met de 41 deelnemers die een slecht privacy statement hebben gezien (M = 3,30, SD = 1,16), scoorden significant beter op vertrouwen $t(77) = 3,2$, p = 0,02.

Variabele 3: Data Protection Officer

Uit de resultaten van de Kolmogorov-Smirnov en de Shapiro Wilk toets blijkt dat de data voor 'de DPO had een goed profiel' en voor 'de DPO had niet een goed profiel' beide normaal is verdeeld. Voor beide testen liggen de p-waardes namelijk (net) hoger dan 0,05, zie ook tabel 19. Dat betekent dat alleen de T-toets wordt uitgevoerd.

Tabel 19: verdeling groepen variabele 3

	Shapiro Wilk		
	Statistic	df	Sig.
De DPO had een goed profiel	0,968	40	0,303
De DPO had niet een goed profiel	0,136	39	0,057

Uit de resultaten van de T-test, zie tabel 20, blijkt dat er geen sprake is van een significant verschil tussen beide opties. Een p-waarde van 0,288 ligt namelijk boven de algemene gewenste waarde van 0,005 en boven de waarde van 0,100 die eventueel voor een experiment gehanteerd zou mogen worden. Er is daarnaast wel sprake van homogeniteit

binnen de varianties, want de p-waarde voor de Levene's test is hoger dan 0,05. Hieruit blijkt dat de T-test als een betrouwbare test gezien kan worden.

Tabel 20: resultaten T-test variabele 3

	Beschrijvend			T-Test			Equal Variances
	N	Mean	Std.Deviation	*t*-value	df	p-value	Levene's Test
De DPO had een goed profiel	40	3,8000	1,09479	1,070	77	0,288	0,464 (Equal variances assumed)
De DPO had niet een goed profiel	39	3,5321	1,13000				

Conclusie

De 40 deelnemers die een goed DPO profiel hebben gezien (M = 3,80, SD = 1,09), vergeleken met de 39 deelnemers die een slecht DPO profiel hebben gezien (M = 3,53, SD = 1,13), scoorden niet significant beter op vertrouwen $t(77) = 1,07$, $p = 0,288$.

4.5 Aanvullende analyses

4.5.1 Verbanden op scenario niveau

Aangezien de varianten van variabelen niet losstaand zijn getoetst, maar altijd als combinatie van verschillende varianten in een scenario, is het interessant om ze ook te bekijken in de context van het onderzoek. Daarom wordt in deze paragraaf gekeken of er een significant verschil is tussen de scenario's. Met behulp van de ANOVA-test is al aangetoond dat er verschil is, maar in deze paragraaf wordt er echt gekeken naar het verschil op scenario niveau. Dit is gedaan met behulp van de T-test. In tabel 21 zijn de uitkomsten schematisch weergegeven in een kruistabel. De kleur groen betekent dat er een significant verschil is tussen beide scenario's, de kleur oranje betekent dat er geen significant verschil is tussen beide scenario's.

Tabel 21: toetsen significantie tussen scenario's

Scenario nummer	1 (11 resp.)	2 (7 resp.)	3 (9 resp.)	4 (12 resp.)	5 (12 resp.)	6 (8 resp.)	7 (9 resp.)	8 (11 resp.)
1 (11 resp.)		T(16)=1,09 P=0,293	T(18)=2,14 P=0,046	T(21)=2,11 P=0,047	T(21)=3,47 P=0,002	T(15,5)=1,14 P=0,272	T(18)=1,84 P=0,082	T(20)=2,54 P=0,02
2 (7 resp.)	T(16)=1,09 P=0,293		T(14)=0,95 P=0,359	T(17)=0,66 P=0,052	T(17)=1,88 P=0,077	T(8,7)=-0,29 P=0,760	T(14)=0,71 P=0,490	T(16)=1,26 P=0,224
3 (9 resp.)	T(18)=2,14 P=0,046	T(14)=0,95 P=0,359		T(19)=-0,59 P=0,560	T(19)=0,54 P=0,596	T(15)=-1,43 P=0,174	T(16)=-0,20 P=0,842	T(18)=0,34 P=0,742
4 (12 resp.)	T(21)=2,11 P=0,047	T(17)=0,66 P=0,052	T(19)=-0,59 P=0,560		T(22)=0,76 P=0,142	T(18)=-1,23 P=0,235	T(19)=0,31 P=0,759	T(21)=1,01 P=0,323
5 (12 resp.)	T(21)=3,47 P=0,002	T(17)=1,88 P=0,077	T(19)=0,54 P=0,596	T(22)=0,76 P=0,142		T(18)=-2,84 P=0,011	T(19)=-0,78 P=0,443	T(21)=-0,10 P=0,918
6 (8 resp.)	T(15,5)=1,14 P=0,272	T(8,7)=-0,29 P=0,760	T(15)=-1,43 P=0,174	T(18)=-1,23 P=0,235	T(18)=-2,84 P=0,011		T(10,6)=1,16 P=0,270	T(13,7)=1,98 P=0,068
7 (9 resp.)	T(18)=1,84 P=0,082	T(14)=0,71 P=0,490	T(16)=-0,20 P=0,842	T(19)=0,31 P=0,759	T(19)=-0,78 P=0,443	T(10,6)=1,16 P=0,270		T(18)=0,53 P=0,601
8 (11 resp.)	T(20)=2,54 P=0,02	T(16)=1,26 P=0,224	T(18)=0,34 P=0,742	T(21)=1,01 P=0,323	T(21)=-0,10 P=0,918	T(13,7)=1,98 P=0,068	T(18)=0,53 P=0,601	

Conclusies verbanden op scenario niveau
Uit tabel 21 is op te maken dat wanneer alle drie de variabelen tegelijkertijd in een goede conditie werden getoond, dit leidde tot meer vertrouwen dan wanneer slechts één variabele in de goede conditie werd getoond. Ook blijkt uit de tabel dat het combineren van bepaalde variabelen leidt tot meer vertrouwen. Het is daarom interessant om verder te onderzoeken of dit ook uit de data blijkt. Hierbij moet wel de kanttekening worden geplaatst dat in paragraaf 4.4.3 al is aangetoond dat er geen significant verschil bestaat tussen het wel en niet hebben van een goede DPO, maar het is wel interessant om te kijken of een DPO in combinatie met andere variabelen wel een significante toegevoegde waarde kan hebben. In paragraaf 4.5.2 wordt hier verder op ingegaan.

4.5.2 Invloed van meerdere goede varianten op vertrouwen
Om te kijken of er een verschil bestaat tussen de scenario's waarbij één goede conditie is getoond en de scenario's waarbij twee goede condities zijn getoond, wordt er nog een aanvullende analyse gedaan. Dit bleek al deels uit paragraaf 4.5.1, maar dat wordt in deze paragraaf dieper onderzocht. Allereerst wordt er gekeken naar de gemiddelden en vervolgens naar de significantie tussen deze gemiddelden.

De scenario's 3, 4 en 5 hebben één goede conditie van een variabele. Gemiddeld scoren deze scenario's samen 3,4 op vertrouwen. De scenario's 2, 6 en 7 hebben twee goede variabelen en scoren gemiddeld 3,8 op vertrouwen In tabel 22 is dit in perspectief geplaatst ten opzichte van 0 goede variabelen en 3 goede variabelen.

Tabel 22: gemiddelde score op vertrouwen per aantal goede varianten

Aantal goede variabelen	Gemiddelde score op vertrouwen
0 goede variabelen (scenario 8)	3,2
1 goede variabele (scenario's 3, 4 en 5)	3,4
2 goede variabelen (scenario's 2, 6 en 7)	3,8
3 goede variabelen (scenario 1)	4,5

Hieruit blijkt dat het scenario waarbij de goede versie van alle variabelen gezamenlijk zijn getoond, nog steeds het hoogste scoort op vertrouwen. Vervolgens scoren de scenario's waarbij twee goede varianten van variabelen zijn getoond het hoogst, dan de scenario's waarbij één goede variabele is getoond en tenslotte het scenario waarbij geen goede varianten van variabelen zijn getoond. Of dit verschil ook significant is te noemen wordt getoetst met behulp van de ANOVA-toets. De resultaten hiervan zijn terug te vinden in tabel 23. Er is gekozen voor de ANOVA-toets omdat er sprake is van het vergelijken van twee of meer groepen op basis van gemiddeldes van deze groepen.

Tabel 23: ANOVA test tussen scenario's

ANOVA					
	Sum of Squares	Df	Mean Square	F	Sig.
BETWEEN GROUPS	13,076	3	4,359	3,910	0,012
WITHIN GROUPS	83,608	75	1,115		
TOTAL	96,684	78			

De resultaten van de ANOVA-toets laten zien dat er een significant verschil is tussen de groepen met 0 goede varianten, 1 goede variant, 2 goede varianten of 3 goede varianten (F(3)=3,910, p = 0,012). Om te kijken tussen welke groepen deze significantie precies zit, wordt er nog gekeken naar de resultaten van de Post-Hoc-Test. De resultaten daarvan zijn weergegeven in tabel 24. Hieruit blijkt dat er vooral een significant verschil zit tussen de scenario's met 0 goede varianten en 3 goede varianten, en tussen de scenario's met 1 goede variant en 3 goede varianten. Ook uit tabel 21 bleek al dat wanneer de goede varianten gezamenlijk werden getoond, dat leidde tot significant meer vertrouwen dan wanneer de variabelen alleen werden getoond (scenario's 1&3, 1&4 en 1&5). Uit tabel 21 bleek ook al dat wanneer alle goede variabelen werden getoond dat dat leidde tot meer vertrouwen dan wanneer er geen enkele goede variabele is getoond (scenario 1&8).

Tabel 24: Post-Hoc test ANOVA tussen scenario's

Multiple Comparisons

Dependent Variable: Vertrouwen_gemiddelde_totaalscore

Tukey HSD

(I) Nummer_Group		Mean Difference (I-J)	Std. Error	Sig.
,00	1,00	-0,20833	0,36759	0,942
	2,00	-0,63920	0,38444	0,351
	3,00	-1,30682*	0,45021	0,025
1,00	,00	0,20833	0,36759	0,942
	2,00	-0,43087	0,28325	0,430
	3,00	-1,09848*	0,36759	0,019
2,00	,00	0,63920	0,38444	0,351
	1,00	0,43087	0,28325	0,430
	3,00	-0,66761	0,38444	0,312
3,00	,00	1,30682*	0,45021	0,025
	1,00	1,09848*	0,36759	0,019
	2,00	0,66761	0,38444	0,312

*. The mean difference is significant at the 0.05 level.

4.5.3 Invloed van variabelen onderling

Tenslotte wordt er nog gekeken of er een verband is tussen de variabelen onderling. Er wordt specifiek gekeken of een variabele aanwezig was in een scenario of niet en of dat invloed had op het vertrouwen van consumenten. Dit is eigenlijk een combinatie tussen de analyses van paragraaf 4.4 en 4.5. Oranje betekent dat er geen significant verschil is gevonden, groen betekent dat er wel een significant verschil is gevonden.

Variabele 1: Keurmerk

Tabel 25: invloed variabelen onderling keurmerk

DE SCENARIO'S	WORDEN GECOMBINEERD BEKEKEN OMDAT.	RESULTATEN
3 EN 8	Alleen in scenario 3 is van alle drie de variabelen alleen de goede variant van het keurmerk getoond. In scenario 8 is van geen enkele variabele een goede variant getoond. Door deze met elkaar te vergelijken wordt bekeken wat het effect is van alleen het hebben van een goede DPO op het vertrouwen van consumenten.	Uit tabel 8 blijkt dat de gemiddelde score op vertrouwen voor scenario 3 (3,40 gemiddeld), hoger ligt dan voor scenario 8 (3,20 gemiddeld). Echter uit tabel 21 blijkt dat er geen significant verschil te ontdekken is tussen deze twee scenario's.
3 EN (4+5)	Alleen in scenario 3 is van alle drie de variabelen alleen de goede variant van het keurmerk getoond. In de scenario's 4 en 5 geldt dat voor de andere twee variabelen de juiste versie is getoond. Door naar deze combinatie te kijken wordt het effect van een Keurmerk bekeken ten opzichte van de andere twee variabelen.	Uit tabel 8 blijkt dat de gemiddelde score op vertrouwen voor scenario 3 (3,40 gemiddeld), overeenkomt met de gemiddelde score van scenario 4 en 5 (3,41 gemiddeld). Uit de T-test blijkt dat er geen significant verschil is tussen scenario 3 en 4 & 5 samen t(-0,36)=31, p=0,971.

2 EN 4	In scenario 2 zijn de goede opties van het keurmerk en de privacy policy getoond, in scenario 4 alleen van de privacy policy. Door deze twee met elkaar te vergelijken wordt gekeken of het keurmerk een versterkend effect heeft op het vertrouwen van consumenten wanneer dat in combinatie met de privacy policy wordt getoond.	Uit tabel 8 blijkt dat de gemiddelde score op vertrouwen voor scenario 2 (3,96 gemiddeld), hoger ligt dan voor scenario 4 (3,67 gemiddeld). Uit tabel 21 blijkt dat er inderdaad een significant verschil is tussen deze beide scenario's.
7 EN 5	In scenario 7 zijn de goede opties van het keurmerk en de DPO getoond, in scenario 5 alleen van de DPO. Door deze twee met elkaar te vergelijken wordt gekeken of het keurmerk een versterkend effect heeft op het vertrouwen van consumenten wanneer dat in combinatie met de DPO wordt getoond.	Uit tabel 8 blijkt dat de gemiddelde score op vertrouwen voor scenario 7 (3,53 gemiddeld), hoger ligt dan voor scenario 5 (3,16 gemiddeld). Uit tabel 21 blijkt echter dat er geen significant verschil is tussen beide scenario's.
1 EN 6	In scenario 1 zijn alle goede varianten van de variabelen getoond, in scenario 6 alleen de goede varianten van de andere twee variabelen en dus niet van het keurmerk. Door deze twee met elkaar te vergelijken wordt gekeken of het toevoegen van een keurmerk effect heeft op het vertrouwen of niet.	Uit tabel 8 blijkt dat de gemiddelde score op vertrouwen voor scenario 1 (4,51 gemiddeld), hoger ligt dan voor scenario 6 (4,09 gemiddeld). Uit tabel 21 blijkt echter dat er geen significant verschil is tussen beide scenario's.

Conclusie variabele 1

Uit de gecombineerde analyses blijkt dat wanneer het keurmerk wordt getoond in combinatie met een goede privacy policy dat dat leidt tot meer vertrouwen van consumenten in een organisatie dan wanneer alleen een goede privacy policy wordt getoond.

Variabele 2: Privacy Policy

Tabel 26: invloed variabelen onderling privacy policy

DE SCENARIO'S	WORDEN GECOMBINEERD BEKEKEN OMDAT.	RESULTATEN
4 EN 8	Alleen in scenario 4 is van alle drie de variabelen alleen de goede variant van de privacy policy getoond. In scenario 8 is van geen enkele variabele een goede variant getoond. Door deze met elkaar te vergelijken wordt bekeken wat het effect is van alleen het hebben van een goed privacy policy op het vertrouwen van consumenten.	Uit tabel 8 blijkt dat de gemiddelde score op vertrouwen voor scenario 4 (3,68 gemiddeld), hoger ligt dan voor scenario 8 (3,20 gemiddeld). Echter uit tabel 21 blijkt dat er geen significant verschil te ontdekken is tussen deze twee scenario's.
4 EN (3+5)	Alleen in scenario 4 is van alle drie de variabelen alleen de goede variant van het privacy policy getoond. In de scenario's 3 en 5 geldt dat voor de andere twee variabelen de juiste versie is getoond. Door naar deze combinatie te kijken wordt het effect van een privacy policy bekeken ten opzichte van de andere twee variabelen.	Uit tabel 8 blijkt dat de gemiddelde score op vertrouwen voor scenario 4 (3,68 gemiddeld), overeenkomt met de gemiddelde score van scenario 3 en 5 (3,28 gemiddeld). Uit de T-test blijkt dat er geen significant verschil is tussen scenario 4 en 3 & 5 samen t(1,193)=31, p=0,242.

2 EN 3	In scenario 2 zijn de goede opties van het keurmerk en de privacy policy getoond, in scenario 3 alleen van het keurmerk. Door deze twee met elkaar te vergelijken wordt gekeken of de privacy policy een versterkend effect heeft op het vertrouwen van consumenten wanneer dat in combinatie met het keurmerk wordt getoond.	Uit tabel 8 blijkt dat de gemiddelde score op vertrouwen voor scenario 2 (3,96 gemiddeld), hoger ligt dan voor scenario 3 (3,40 gemiddeld). Uit tabel 21 blijkt dat er geen significant verschil is tussen deze beide scenario's.
6 EN 5	In scenario 6 zijn de goede opties van de privacy policy en de DPO getoond, in scenario 5 alleen van de DPO. Door deze twee met elkaar te vergelijken wordt gekeken of de privacy policy een versterkend effect heeft op het vertrouwen van consumenten wanneer dat in combinatie met de DPO wordt getoond.	Uit tabel 8 blijkt dat de gemiddelde score op vertrouwen voor scenario 6 (4,09 gemiddeld), hoger ligt dan voor scenario 5 (3,16 gemiddeld). Uit tabel 21 blijkt echter dat er inderdaad een significant verschil is tussen beide scenario's.
1 EN 7	In scenario 1 zijn alle goede varianten van de variabelen getoond, in scenario 7 alleen de goede varianten van de andere twee variabelen en dus niet van het privacy policy. Door deze twee met elkaar te vergelijken wordt gekeken of het toevoegen van de privacy policy effect heeft op het vertrouwen of niet.	Uit tabel 8 blijkt dat de gemiddelde score op vertrouwen voor scenario 1 (4,51 gemiddeld), hoger ligt dan voor scenario 7 (3,53 gemiddeld). Uit tabel 21 blijkt echter dat er inderdaad een significant verschil is tussen beide scenario's.

Conclusie variabele 2

Uit de gecombineerde analyses blijkt dat een goede privacy policy in combinatie met een goede DPO tot meer vertrouwen leidt bij consumenten dan wanneer alleen een goede DPO aanwezig is. Ook blijkt het toevoegen van een privacy policy tot meer vertrouwen leidt als dat wordt getoond samen met een goede DPO en een keurmerk dan wanneer een goede DPO en de aanwezigheid van een keurmerk alleen worden getoond.

Variabele 3: Data Protection Officer

Tabel 27: invloed variabelen onderling DPO

DE SCENARIO'S	WORDEN GECOMBINEERD BEKEKEN OMDAT.	RESULTATEN
5 EN 8	Alleen in scenario 5 is van alle drie de variabelen alleen de goede variant van de DPO getoond. In scenario 8 is van geen enkele variabele een goede variant getoond. Door deze met elkaar te vergelijken wordt bekeken wat het effect is van alleen het hebben van een goede DPO op het vertrouwen van consumenten.	Uit tabel 8 blijkt dat de gemiddelde score op vertrouwen voor scenario 5 (3,16 gemiddeld), lager ligt dan voor scenario 8 (3,20 gemiddeld). Echter uit tabel 21 blijkt dat er geen significant verschil te ontdekken is tussen deze twee scenario's.
5 EN (3+4)	Alleen in scenario 5 is van alle drie de variabelen alleen de goede variant van de DPO getoond. In de scenario's 3 en 4 geldt dat voor de andere twee variabelen de juiste versie is getoond. Door naar deze combinatie te kijken	Uit tabel 8 blijkt dat de gemiddelde score op vertrouwen voor scenario 5 (3,28 gemiddeld), overeenkomt met de gemiddelde score van scenario 4 en 6 (3,28 gemiddeld). Uit de T-test blijkt dat er geen significant verschil is tussen scenario 5 en 3 & 4 samen t(-1,157)=31, p=0,256.

	wordt het effect van een Keurmerk bekeken ten opzichte van de andere twee variabelen.	
4 EN 6	In scenario 6 zijn de goede opties van de privacy policy en de DPO getoond, in scenario 4 alleen van de privacy policy. Door deze twee met elkaar te vergelijken wordt gekeken of de DPO een versterkend effect heeft op het vertrouwen van consumenten wanneer dat in combinatie met de privacy policy wordt getoond.	Uit tabel 8 blijkt dat de gemiddelde score op vertrouwen voor scenario 4 (3,68 gemiddeld), lager ligt dan voor scenario 6 (4,09 gemiddeld). Uit tabel 21 blijkt dat er geen significant verschil is tussen deze beide scenario's.
7 EN 3	In scenario 7 zijn de goede opties van het keurmerk en de DPO getoond, in scenario 3 alleen van het keurmerk. Door deze twee met elkaar te vergelijken wordt gekeken of de DPO een versterkend effect heeft op het vertrouwen van consumenten wanneer dat in combinatie met het keurmerk wordt getoond.	Uit tabel 8 blijkt dat de gemiddelde score op vertrouwen voor scenario 7 (3,53 gemiddeld), hoger ligt dan voor scenario 3 (3,40 gemiddeld). Uit tabel 21 blijkt echter dat er geen significant verschil is tussen beide scenario's.
1 EN 2	In scenario 1 zijn alle goede varianten van de variabelen getoond, in scenario 2 alleen de goede varianten van de andere twee variabelen en dus niet van de DPO. Door deze twee met elkaar te vergelijken wordt gekeken of het toevoegen van een DPO effect heeft op het vertrouwen of niet.	Uit tabel 8 blijkt dat de gemiddelde score op vertrouwen voor scenario 1 (4,51 gemiddeld), hoger ligt dan voor scenario 2 (3,96 gemiddeld). Uit tabel 21 blijkt echter dat er geen significant verschil is tussen beide scenario's.

Conclusie variabele 3
Uit de gecombineerde analyses blijkt dat het toevoegen van een goede DPO aan de andere vormen die zijn onderzocht, statistisch gezien niet bijdraagt aan een verhoogd vertrouwen van consumenten in een organisatie.

5. Conclusies, discussie & aanbevelingen

In dit laatste hoofdstuk wordt stilgestaan bij de conclusies, discussie en aanbevelingen en beperkingen. In de paragraaf conclusies wordt allereerst een samenvatting weergegeven van de belangrijkste conclusies die voortvloeien uit het onderzoek. Vervolgens zal er in de paragraaf discussie worden ingegaan op de relatie tussen de onderzoeksresultaten en het theoretisch kader. In de paragraaf aanbevelingen worden aanbevelingen gedaan voor vervolgonderzoek. Tenslotte wordt in de paragraaf beperkingen, ingegaan op de beperkingen van het onderzoek.

5.1 Conclusies

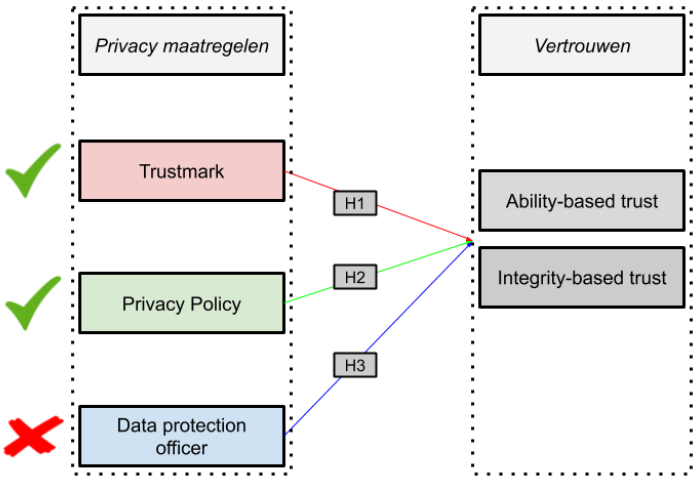
De hoofdvraag van dit onderzoek luidt als volgt: *Wat is de invloed van het privacy beleid van online bedrijven op de vertrouwensperceptie van consumenten?*

Dit onderzoek toont aan dat een goede privacy policy en een privacy keurmerk, bijdragen aan het vertrouwen van consumenten in online bedrijven. Ook laat het onderzoek zien dat een data protection officer (functionaris gegevensbescherming) niet bijdraagt aan het vertrouwen

van consumenten in online bedrijven. In afbeelding 3 is dit schematisch weergegeven. Concreet betekent dit het volgende voor de drie hypotheses die vooraf zijn geformuleerd:

Hypothese 1: Trustmarks
Het onderzoek bevestigt dat een zichtbare trustmark een positieve invloed heeft op het vertrouwen van Nederlandse consumenten in e-commerce bedrijven. Daarmee wordt hypothese 1 aangenomen.

Hypothese 2: Inhoudelijke privacy policy
Het onderzoek bevestigt dat een inhoudelijk goede privacy policy een positieve invloed heeft op het vertrouwen van Nederlandse consumenten in e-commerce bedrijven. Daarmee wordt hypothese 2 aangenomen.



Figuur 3: schematische weergave resultaten onderzoek

Hypothese 3: Data Protection Officer
Het onderzoek ontkracht dat het hebben van een DPO een positieve invloed heeft op het vertrouwen van Nederlandse consumenten in e-commerce bedrijven. Hypothese 3 wordt daarom verworpen.

Aanvullend onderzoek toont aan dat ability-based trust en integrity-based trust gezamenlijk het concept vertrouwen vormen en dat daartussen in dit onderzoek geen onderscheid wordt gezien. Ook toont het onderzoek aan dat sommige variabelen gezamenlijk tot meer vertrouwen leiden dan wanneer ze alleen getoond worden. De combinaties die leiden tot meer vertrouwen zijn:

- Privacy policy & keurmerk vergeleken met alleen een goede privacy policy.
- Privacy policy & goede DPO vergeleken met alleen een goede DPO.
- Privacy policy & goede DPO + keurmerk vergeleken met alleen een goede DPO en een zichtbaar keurmerk.

5.2 Discussie
Uit het onderzoek blijkt dat twee van de drie variabelen inderdaad bijdragen aan het vertrouwen van consumenten in online winkels en dat variabelen gecombineerd soms leiden tot meer vertrouwen dan wanneer ze als losse elementen worden gezien. In deze paragraaf worden de resultaten per variabele besproken en gekoppeld aan de theorie zoals besproken in hoofdstuk 2.

5.2.1 Keurmerk
Uit eerdere onderzoeken, waaronder uit die van Liu et al. (2005), Aiken en Boush (2006) en Thompson et al. (2019) bleek al dat het hebben van een keurmerk, invloed heeft op het vertrouwen van consumenten in organisaties. Echter zijn deze onderzoeken allemaal uitgevoerd in andere landen en in een andere context en dus niet gezamenlijk bekeken met een DPO en een Privacy Policy zoals in dit onderzoek. Uit de onderzoeken die al gedaan zijn, bleek dat het hebben van een keurmerk vaak de grootste invloed had op vertrouwen ten

opzichte van de andere twee variabelen die zijn getoetst. Uit dit onderzoek komt dat deels terug wanneer er wordt gekeken naar de combinatie tussen het keurmerk en een privacy policy. En keurmerk en een privacy policy leidt namelijk tot meer vertrouwen dan wanneer een goede privacy policy alleen wordt getoond. Verder blijkt uit dit onderzoek wel dat een keurmerk op zich leidt tot meer vertrouwen bij consumenten wat, op basis van de eerdere onderzoeken, ook te verwachten was en dat een keurmerk dus ook bij de Nederlandse consument leidt tot meer vertrouwen in organisaties.

5.2.2 Privacy Policy

Door Wu et al. (2012) en Liu et al. (2005) is eerder onderzoek gedaan naar de relatie tussen vertrouwen en een privacy policy. In hun onderzoek is een verband gevonden tussen de inhoud van een privacy policy en de mate van vertrouwen en ook is er gekeken naar welke elementen een goede privacy policy moet voldoen. Deze bevindingen zijn gebruikt om de privacy policy's in dit onderzoek vorm te geven. Dit onderzoek toont de privacy policy in combinatie met andere variabelen en in een andere culturele setting dan de hiervoor genoemde onderzoeken. De resultaten van dit onderzoek laten zien dat er een positief verband is tussen een goede privacy policy en vertrouwen. Dit ligt in lijn met de voorgaande onderzoeken aangezien deze als basis zijn gebruikt. Echter was het de vraag of het culturele aspect van invloed zou zijn op de resultaten, aangezien voor dit onderzoek de Nederlandse populatie is gebruikt en in de voorgaande onderzoeken niet. Dat blijkt niet het geval te zijn. Ook laat dit onderzoek zien dat een goede privacy policy een versterkend effect heeft op vertrouwen op het moment dat het getoond wordt in combinatie met een goede DPO dan wanneer een goede DPO alleen wordt getoond.

5.2.3. Data Protection Officer

Voor zover bekend is er nog niet eerder onderzoek gedaan naar het effect van de aanwezigheid van een DPO binnen een organisatie op het vertrouwen van consumenten. In een recent onderzoek van Recio (2017) wordt er een relatie verondersteld, aangezien de DPO bijdraagt aan de accountability van een organisatie en accountability zouden leiden tot vertrouwen. Zij suggereren dit in het onderzoek, maar tonen het niet wetenschappelijk aan. Daarom kon voor deze variabele niet worden teruggevallen op reeds bestaande literatuur voor de bepaling van 'goede' en 'minder goede' varianten van variabelen. Er is daarom gekozen om vanuit de praktijk te bepalen wat een goede DPO zou kunnen zijn en vervolgens is daar een vertaling van gemaakt van een minder goede DPO. De vraag is of dat succesvol is geweest. Zoals is terug te lezen in hoofdstuk 4, zijn er geen statistische verbanden gevonden tussen een goede DPO en het vertrouwen van consumenten. Een mogelijke verklaring hiervoor kan worden gevonden in het gegeven dat vooraf niet onderzocht is bij consumenten wat zij vinden waaraan een goede DPO moet voldoen, maar dat dit is bepaald op basis van vacatures en huidige profielen. Dat is erg vanuit de organisatie geredeneerd, terwijl dit onderzoek zich juist richt op consumenten. Dat geldt eigenlijk ook voor de functie van DPO op zich. Daarnaast is het een vrij nieuwe functie binnen organisaties waardoor consumenten mogelijk niet voldoende op de hoogte zijn wat deze functie precies inhoudt en wat de waarde van deze functie is. Dit is wel tijdens het afnemen van de enquête beschreven, maar of respondenten dat ook echt hebben gelezen is niet bekend. Een laatste verklaring zou kunnen zijn dat het profiel van de DPO altijd als laatste variabele is getoond aan de respondenten en dat respondenten hun oordeel over de organisatie al klaar hadden na het zien van de eerste twee variabelen.

Nota bene: Het feit dat uit dit onderzoek is gebleken dat een goede DPO geen invloed heeft op het vertrouwen van consumenten in organisaties, neemt vanzelfsprekend niet weg dat een goede DPO van belang is voor de organisatie.

5.2.4 Variabelen gecombineerd

Tenslotte blijkt uit het onderzoek dat het combineren van variabelen kan leiden tot meer vertrouwen dan wanneer een variabele losstaand is getoond. Dit is vooraf niet uit het literatuuronderzoek verondersteld, maar het bleek wel uit de resultaten. Logisch beredeneerd is het ook niet gek dat twee variabelen leiden tot meer vertrouwen dan wanneer een variabele op zichzelf staat. Hierin is het met name interessant dat het toevoegen van een goede privacy policy en het tonen van een keurmerk een grote rol spelen. Dit is weer in lijn met de bevinding dat een DPO statistisch gezien niet leidt tot meer vertrouwen, waardoor het toevoegen van een DPO aan een van de andere variabelen geen verdere invloed heeft.

5.3 Aanbevelingen

In deze paragraaf worden aanbevelingen gedaan voor vervolgonderzoek en worden aanbevelingen gedaan voor de praktijk en hoe dit onderzoek daarin kan worden toegepast.

5.3.1 Aanbevelingen voor vervolgonderzoek

Dit onderzoek levert een bijdrage aan het inzicht in de relatie tussen vertrouwen en het privacy beleid van organisaties in de context van de AVG. In deze context worden er aanbevelingen gedaan voor vervolgonderzoek.

Aangezien is gebleken dat een goede DPO niet van invloed is op het vertrouwen van consumenten in organisaties, is het interessant om hier verder onderzoek naar te doen. Niet alleen omdat hier nog maar zeer beperkt onderzoek naar is gedaan, maar ook omdat bedrijven sinds de invoering van de AVG in bepaalde gevallen verplicht zijn om een DPO aan te stellen. Zijn consumenten bijvoorbeeld bekend met een DPO? Zien ze er de meerwaarde van in? En wat is eigenlijk de definitie van een goede DPO? Willen consumenten eigenlijk wel geconfronteerd worden met de functie van de DPO of hechten ze er meer waarde aan dat hetgeen waarvoor een DPO is aangesteld, goed gebeurt? Dit zijn allemaal nog open vragen die in dit onderzoek niet worden beantwoord.

Ten tweede is het interessant om de tekst van de privacy policy onder de loep te nemen. Het benoemen van bepaalde onderdelen in de privacy policy is één ding, maar het is ook interessant om te kijken of het vertrouwen wordt beïnvloed door de manier waarop het onderdeel in de privacy policy staat omschreven. Dit gaat dus meer over het linguïstische aspect van de privacy policy.

Tenslotte zijn de varianten in dit onderzoek heel zichtbaar geweest voor de respondenten. Ze hebben de afbeeldingen op groot formaat op hun scherm bekeken en ze werden ‘gedwongen’ om ze te zien. Het zou interessant kunnen zijn om dit onderzoek te herhalen in een wat meer natuurlijkere/praktische setting waarbij de respondenten bijvoorbeeld navigeren over een website met een bepaalde taak die niet is gerelateerd aan het onderzoek, en dat dan wordt bekeken of ze überhaupt de privacy policy lezen of letten op een keurmerk. Nu werd

verondersteld dat ze dat doen, maar de vraag is of ze dat in een wat minder klinische setting ook echt doen.

5.3.2 Aanbevelingen voor de praktijk

Allereerst toont dit onderzoek aan dat het voor webwinkels loont om te investeren in een goede privacy policy en, wanneer dit in de toekomst voor Nederland op de markt komt, in een AVG-keurmerk. Maar op dit moment is er nog geen officieel privacy keurmerk voor organisaties beschikbaar. Een ander veelgehoorde opmerking, tevens ook een onderwerp waar onderzoek naar is gedaan door bijvoorbeeld Gindin (2009), is dat privacy statements nauwelijks gelezen worden. De vraag is dus wat praktisch gezien de toegevoegde waarde is van dit onderzoek en wat er vanuit de praktijk nodig is om met de resultaten aan de slag te kunnen.

Ondanks dat organisaties zich wel eens afvragen voor wie ze het privacy statement eigenlijk schrijven, aangezien maar weinig mensen het zouden lezen, is het investeren in een goede privacy policy echt de moeite waard. Dit onderzoek laat zien dat een goede privacy policy bijdraagt aan het vertrouwen van de mensen die het lezen. Niet investeren in een goede privacy policy zou het vertrouwen kunnen schaden van de mensen die lezen wat in het uiterste geval kan leiden tot het verliezen van omzet.

Zoals eerder besproken is in Nederland op dit moment nog geen officieel keurmerk voor organisaties die voldoen aan de AVG. The European Union Agency for Network and Information Security (ENISA) heeft de Europese Unie al geadviseerd om een soort accreditatiesysteem op te zetten om organisaties te kunnen beoordelen op hun privacy beleid (ENISA, 2017), met als resultaat een keurmerk of certificaat op het moment dat een organisatie hieraan voldoet. Echter tot op heden is hieraan nog weinig invulling gegeven. Juist omdat een dergelijk systeem nog niet bestaat, maar het niet tijdig reguleren daarvan wel zou kunnen zorgen voor een wildgroei aan keurmerken en daarmee gepaard gaande audits, is het voor de Europese Unie of de Autoriteit Persoonsgegevens een goed moment om hiervoor de kaders te schetsen. Dit onderzoek laat in ieder geval zien dat het voor bedrijven een toegevoegde waarde heeft op het vertrouwen wat consumenten in hun hebben, op het moment dat ze via een keurmerk kunnen laten zien dat ze voldoen aan de voorwaarden van de AVG. De inzichten van dit onderzoek kunnen daarom een nieuwe stimulans geven aan deze ontwikkeling.

Zowel het keurmerk als de privacy policy kennen dus wat beperkingen in hun praktische toepassing, maar ze zijn wel aan elkaar gewaagd. Want zonder goede privacy policy zal er vermoedelijk geen keurmerk worden afgegeven, maar zonder zichtbaar keurmerk is het de vraag of consumenten goed kunnen inschatten hoe de organisatie omgaat met hun persoonsgegevens. Uit het onderzoek blijkt dat een groot deel van de respondenten veel waarde hecht aan hoe organisaties omgaan met hun persoonsgegevens dus de invulling daarvan is wel degelijk van belang. De oplossing zou kunnen liggen in het gecombineerd toepassen van beide aspecten. Het onderzoek laat namelijk zien dat deze combinatie leidt tot een hogere gemiddelde score op vertrouwen dan wanneer beide aspecten los worden getoond. Bovendien zou een keurmerk en een privacy policy door alle organisaties ingezet kunnen worden. Dat geldt niet voor een DPO aangezien een DPO volgens de wet niet voor alle organisaties verplicht is.

5.4 Beperkingen

Ondanks dat vooraf goed is nagedacht over de aanleiding, opbouw en uitvoering van het onderzoek, zijn er beperkingen aan dit onderzoek en zijn er onderdelen die achteraf anders gedaan hadden moeten worden. In deze paragraaf wordt hierop gereflecteerd.

Allereerst is het onderzoek uitgevoerd binnen de kennissenkring van de onderzoeker, omwille van tijd en gemak, waardoor er sprake was van een convenience sample. Dit op zich kan een bias zijn voor de resultaten van het onderzoek, aangezien het over het algemeen dezelfde type mensen zijn die in deze kennissenkring zitten. Het was vooraf bekend dat dit een van de beperkingen van een convenience sample is, namelijk dat er niet echt gestuurd kan worden op een perfecte sample van respondenten zoals dat bij betaalde onderzoeken gedaan kan worden bijvoorbeeld. De kennissen hebben het onderzoek wel weer verder verspreid in hun kringen dus de resultaten zijn niet alleen maar van bekenden van de onderzoeker, maar ze zijn er wel aan gerelateerd. De kennissenkring van de onderzoeker bestaat voornamelijk uit jongeren, wat ook blijkt uit de resultaten. Bijna 40% van de respondenten is tussen de 25 en 34 jaar. Dit hoeft geen belemmering te zijn, maar het is ook geen volledige afspiegeling van de populatie zoals vooraf was gewenst. Bij de interpretatie van de resultaten is het daarom belangrijk dat ze dus in het licht moeten worden gezien dat het de resultaten zijn gebaseerd op een merendeel jonge populatie. Het is dus niet het resultaat van de volledige populatie die online shopt.

Een ander belangrijk punt is dat voor de vormgeving van het minder goede privacy statement gebruik is gemaakt van een reeds bestaand privacy statement die bij verschillende gemeentes wordt gebruikt. Om aan de voorwaarden te voldoen van een minder goed privacy statement, zijn de elementen die een privacy statement tot een goed privacy statement, weggelaten uit het reeds bestaande privacy statement. Hierdoor bleven elementen over die het volgens de literatuur minder goed zouden doen. Deze zijn gecombineerd en wat ingekort en zo is het minder goede privacy statement ontstaan. Maar, de elementen die overbleven zijn meteen ook elementen die tekstueel minder positief geformuleerd waren. De elementen die zijn gebruikt voor een goed privacy statement waren over het algemeen positiever geformuleerd en kunnen daardoor betrouwbaarder overkomen dan de elementen van het minder goede privacy statement. Hierdoor zou de respondent mogelijk gestuurd kunnen zijn. Dit had voorkomen kunnen worden door de elementen van de minder goede privacy policy positiever te verwoorden zodat het tekstuele element geen rol zou kunnen spelen. Maar om zo dicht mogelijk bij de werkelijkheid te blijven is er bij de opzet van het onderzoek ook bewust voor gekozen om het privacy statement qua inhoud niet te veel te veranderen. Het is belangrijk om met dit gegeven rekening te houden bij de interpretatie van de resultaten.

Een andere beperking aan het onderzoek was dat er op het moment van onderzoeken nog geen literatuur beschikbaar was over een goede DPO, zoals bij de overige twee variabelen wel het geval is geweest. Daarom is er voor dit onderzoek een poging gedaan om op basis van de praktijk zelf criteria te formuleren waaraan een goede DPO moet voldoen. Hoe dat precies is gedaan, is te lezen in bijlage 3. Omdat die eerdere validatie ontbreekt kan het zijn dat er ten onrechte al wordt geconcludeerd dat een DPO geen invloed heeft op het vertrouwen van consumenten in webwinkels. Zoals ook is gesuggereerd is verder onderzoek nodig naar de relatie tussen DPO en vertrouwen.

Bibliografie

Abedjan, Z., Golab, L., & Naumann, F. (2015). Profiling relational data: a survey. *The VLDB Journal, 24*(4), 557-581.

Aiken, D., & Boush, D. (2006). Trustmarks, objective-source ratings, and implied investments in advertising: investigating online trust and the context-specific nature of internet signals. *Journal of the Academy of Marketing Science, 34*(3), 308-323.

Aiken, D., Osland, G., Liu, B., & Mackoy, R. (2003). Developing internet consumer trust: exploring trustmarks as third-party signals. *Marketing theory and applications, 14*, 145-146.

Aldrich, H. E., & Fiol, C. M. (1994). Fools rush in? The institutional context of industry creation. *Academy of management review, 19*(4), 645-670.

Autoriteit Persoonsgegevens. (2019a). AP waarschuwt voor misleidend AVG-keurmerk. Retrieved from https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-waarschuwt-voor-misleidend-avg-keurmerk

Autoriteit Persoonsgegevens. (2019b). Functionaris gegevensbescherming (FG). Retrieved from https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/functionaris-gegevensbescherming-fg

Autoriteit Persoonsgegevens. (2019c). Nederland maakt zich zorgen over privacy. Retrieved from https://autoriteitpersoonsgegevens.nl/nl/nieuws/nederland-maakt-zich-zorgen-over-privacy

Axinte, S.-D., Petrică, G., & Bacivarov, I. (2018). GDPR Impact on Company Management and Processed Data. *Calitatea, 19*(165), 150-153.

Ayala-Rivera, V., & Pasquale, L. (2018). *The grace period has ended: An approach to operationalize GDPR requirements.* Paper presented at the 2018 IEEE 26th International Requirements Engineering Conference (RE).

Bachmann, R., & Inkpen, A. C. (2011). Understanding institutional-based trust building processes in inter-organizational relationships. *Organization Studies, 32*(2), 281-301.

Beldad, A. D., De Jong, M., & Steehouder, M. F. (2009). When the bureaucrat promises to safeguard your online privacy: Dissecting the contents of privacy statements on Dutch municipal websites. *Government Information Quarterly, 26*(4), 559-566.

Bigley, G. A., & Pearce, J. L. (1998). Straining for shared meaning in organization science: Problems of trust and distrust. *Academy of management review, 23*(3), 405-421.

Brown, T. (2015). *Confirmatory factor analysis for applied research*: Guilford publications.

Brown, T., & Dacin, P. (1997). The company and the product: Corporate associations and consumer product responses. *Journal of marketing, 61*(1), 68-84.

Carpenter, V. L., & Feroz, E. H. (2001). Institutional theory and accounting rule choice: an analysis of four US state governments' decisions to adopt generally accepted accounting principles. *Accounting, organizations and society, 26*(7-8), 565-596.

Chomeya, R. (2010). Quality of psychology test between Likert scale 5 and 6 points. *Journal of Social Sciences, 6*(3), 399-403.

Chyung, S. Y., Roberts, K., Swanson, I., & Hankinson, A. (2017). Evidence-based survey design: The use of a midpoint on the Likert scale. *Performance Improvement, 56*(10), 15-23.

Connelly, B. L., Crook, T. R., Combs, J. G., Ketchen Jr, D. J., & Aguinis, H. (2018). Competence- and integrity-based trust in interorganizational relationships: Which matters more? *Journal of Management, 44*(3), 919-945.

De, S. J., & Métayer, D. L. (2016). Privacy risk analysis. *Synthesis Lectures on Information Security, Privacy, & Trust, 8*(3), 1-133.

Deephouse, D. L., & Carter, S. M. (2005). An examination of differences between organizational legitimacy and organizational reputation. *Journal of management Studies, 42*(2), 329-360.

Doney, P. M., & Cannon, J. P. (1997). An examination of the nature of trust in buyer–seller relationships. *Journal of marketing, 61*(2), 35-51.

EDPS. (2016). The History of the General Data Protection Regulation. Retrieved from https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

ENISA. (2017). *Recommendations on European Data Protection Certification*. Retrieved from https://www.enisa.europa.eu/news/enisa-news/enisa-report-concepts-and-recommendations-on-european-data-protection-certification-mechanisms

Field, A. (2009). Discovering Statistics Using SPSS. In (3rd ed.): Sage Publications.

Flavián, C., & Guinalíu, M. (2006). Consumer trust, perceived security and privacy policy: three basic elements of loyalty to a web site. *Industrial management & Data systems, 106*(5), 601-620.

Fombrun, C., & Shanley, M. (1990). What's in a name? Reputation building and corporate strategy. *Academy of management Journal, 33*(2), 233-258.

Garbarino, E., & Johnson, M. S. (1999). The different roles of satisfaction, trust, and commitment in customer relationships. *Journal of marketing, 63*(2), 70-87.

Garland, R. (1991). The mid-point on a rating scale: Is it desirable. *Marketing bulletin, 2*(1), 66-70.

Gellman, R., & Dixon, P. (2011). *Online privacy: a reference handbook*: ABC-CLIO.

Gindin, S. E. (2009). Nobody reads your privacy policy or online contract: Lessons learned and questions raised by the FTC's action against Sears. *Nw. J. Tech. & Intell. Prop., 8*, 1.

Hannan, M. T., & Freeman, J. (1986). *Where do organizational forms come from?* Paper presented at the Sociological forum.

Harris, L. C., & Goode, M. M. (2004). The four levels of loyalty and the pivotal role of trust: a study of online service dynamics. *Journal of retailing, 80*(2), 139-158.

Hills, P., & Argyle, M. (2002). The Oxford Happiness Questionnaire: a compact scale for the measurement of psychological well-being. *Personality and individual differences, 33*(7), 1073-1082.

Hong, I. B., & Cho, H. (2011). The impact of consumer trust on attitudinal loyalty and purchase intentions in B2C e-marketplaces: Intermediary trust vs. seller trust. *International Journal of Information Management, 31*(5), 469-479.

Jacoby, J., & Matell, M. S. (1971). Three-point Likert scales are good enough. In: SAGE Publications Sage CA: Los Angeles, CA.

Jayasinghe, U., Lee, G. M., & MacDermott, A. (2018). *Trust-based data controller for personal information management.* Paper presented at the 2018 International Conference on Innovations in Information Technology (IIT).

Kemp, R. (2007). Privacy. *Library Hi Tech, 25*(1), 58-78. doi:10.1108/07378830710735867

Kim, P., Ferrin, D. L., Cooper, C. D., & Dirks, K. T. (2004). Removing the shadow of suspicion: the effects of apology versus denial for repairing competence-versus integrity-based trust violations. *Journal of applied psychology, 89*(1), 104.

Kim, S.-H. (2010). The influence of likert scale format on response result, validity, and reliability of scale-using scales measuring economic shopping orientation. *Journal of the Korean Society of Clothing and Textiles, 34*(6), 913-927.

King, B. G., & Whetten, D. A. (2008). Rethinking the relationship between reputation and legitimacy: A social actor conceptualization. *Corporate Reputation Review, 11*(3), 192-207.

Krithikadatta, J. (2014). Normal distribution. *Journal of conservative dentistry: JCD, 17*(1), 96.

Leung, S.-O. (2011). A comparison of psychometric properties and normality in 4-, 5-, 6-, and 11-point Likert scales. *Journal of Social Service Research, 37*(4), 412-421.

Liu, C., Marchewka, J. T., Lu, J., & Yu, C.-S. (2005). Beyond concern—a privacy-trust-behavioral intention model of electronic commerce. *Information & Management, 42*(2), 289-304.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of management review, 20*(3), 709-734.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002a). Developing and validating trust measures for e-commerce: An integrative typology. *Information systems research, 13*(3), 334-359.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002b). The impact of initial consumer trust on intentions to transact with a web site: a trust building model. *The Journal of Strategic Information Systems, 11*(3-4), 297-323.

Metlay, D. (2013). Institutional trust and confidence: A journey into a conceptual quagmire. In *Social trust and the management of risk* (pp. 114-130): Routledge.

Meyer, J. W., & Rowan, B. (1977). Institutionalized organizations: Formal structure as myth and ceremony. *American journal of sociology, 83*(2), 340-363.

Milne, G. R., & Boza, M. E. (1999). Trust and concern in consumers' perceptions of marketing information management practices. *Journal of interactive marketing, 13*(1), 5-24.

Oliver, C. (1991). Strategic responses to institutional processes. *Academy of management review, 16*(1), 145-179.

Park, J., Gunn, F., & Han, S.-L. (2012). Multidimensional trust building in e-retailing: Cross-cultural differences in trust formation and implications for perceived risk. *Journal of Retailing and Consumer Services, 19*(3), 304-312.

Pelteret, M., & Ophoff, J. (2016). A review of information privacy and its importance to consumers and organizations. *Informing Science: The International Journal of an Emerging Transdiscipline, 19*, 277-301.

Pfeffer, J., & Salancik, G. R. (2003). *The external control of organizations: A resource dependence perspective*: Stanford University Press.

Politou, E., Alepis, E., & Patsakis, C. (2018). Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *Journal of Cybersecurity, 4*(1), tyy001.

Preston, C. C., & Colman, A. M. (2000). Optimal number of response categories in rating scales: reliability, validity, discriminating power, and respondent preferences. *Acta psychologica, 104*(1), 1-15.

Recio, M. (2017). Data Protection Officer: The Key Figure to Ensure Data Protection and Accountability. *Eur. Data Prot. L. Rev., 3*, 114.

Reichheld, F. F., & Schefter, P. (2000). E-loyalty: your secret weapon on the web. *Harvard business review, 78*(4), 105-113.

Richardson, A. J., & Joshi, A. (1997). *Exploring the empirical relationship between legitimacy and efficiency: models and methods.* Paper presented at the Interdisciplinary Perspectives on Accounting Conference, Manchester, UK.

Roberts, J. M., & Gregor, T. (2017). Privacy: A cultural view. In *Privacy and Personality* (pp. 199-225): Routledge.

Saunders, M., Lewis, P., & Thornhill, A. (2016). Research Methods for Business students.(ed. 7 th) Harlow. In: Pearson Education Limited.

Schermer, B., Hagenauw, D., & Falot, N. (2018). *Handleiding Algemene verordening gegevensbescherming*. Retrieved from

Scott, W. R. (1987). Organizations: Rational, natural, and open systems.

Scribber. (2014). Wat is een conceptueel model? Retrieved from https://www.scribbr.nl/scriptie-structuur/conceptueel-model

Simpson, D. (2016). The Use of Big Data: Benefits, Risks, and Differential Pricing Issues. *Nueva York: Nova Science Publisher*.

Sparling, E. I. G., & Sen, S. (2010). Cognitive load of rating scales.

Suchman, M. C. (1995). Managing legitimacy: Strategic and institutional approaches. *Academy of management review, 20*(3), 571-610.

Sullivan, Y. W., & Kim, D. J. (2018). Assessing the effects of consumers' product evaluations and trust on repurchase intention in e-commerce environments. *International Journal of Information Management, 39*, 199-219.

Terwel, B. W., Harinck, F., Ellemers, N., & Daamen, D. D. (2009). Competence-based and integrity-based trust as predictors of acceptance of carbon dioxide capture and storage (CCS). *Risk Analysis: An International Journal, 29*(8), 1129-1140.

Thompson, F. M., Tuzovic, S., & Braun, C. (2019). Trustmarks: Strategies for exploiting their full potential in e-commerce. *Business Horizons, 62*(2), 237-247.

Van Dyke, T. P., Midha, V., & Nemati, H. (2007). The effect of consumer privacy empowerment on trust and privacy concerns in e-commerce. *Electronic Markets, 17*(1), 68-81.

Vance, A. O. (2009). Trusting IT artifacts: How trust affects our use of technology.

VanVoorhis, C. W., & Morgan, B. L. (2007). Understanding power and rules of thumb for determining sample sizes. *Tutorials in quantitative methods for psychology, 3*(2), 43-50.

Velicer, W. F., & Jackson, D. N. (1990). Component analysis versus common factor analysis: Some issues in selecting an appropriate procedure. *Multivariate behavioral research, 25*(1), 1-28.

Verhoef, P., Kooge, E., & Walk, N. (2016). *Creating value with big data analytics: Making smarter marketing decisions*: Routledge.

Westin, A. F. (1968). Privacy and freedom. *Washington and Lee Law Review, 25*(1), 166.

Wood, D. J. (1991). Corporate social performance revisited. *Academy of management review, 16*(4), 691-718.

Wu, K.-W., Huang, S. Y., Yen, D. C., & Popova, I. (2012). The effect of online privacy policy on consumer privacy concern and trust. *Computers in human behavior, 28*(3), 889-897.

Xie, Y., & Peng, S. (2009). How to repair customer trust after negative publicity: The roles of competence, integrity, benevolence, and forgiveness. *Psychology & Marketing, 26*(7), 572-589.

Yang, M.-H., Lin, B., Chandlrees, N., & Chao, H.-Y. (2009). The effect of perceived ethical performance of shopping websites on consumer trust. *Journal of computer information systems, 50*(1), 15-24.

Yap, B. W., & Sim, C. H. (2011). Comparisons of various types of normality tests. *Journal of Statistical Computation and Simulation, 81*(12), 2141-2155.

Bijlage 1: Zoekstrategie

In deze bijlage wordt de strategie beschreven die is gebruikt om aan de artikelen voor deze scriptie te komen.

Fase 1: bepalen zoekwoorden

Aan de hand van de voorlopige hoofdvraag die is geformuleerd, zijn zoektermen bepaald die relevant kunnen zijn voor het onderzoek. De hoofdvraag is uitgesplitst in drie verschillende zoekpaden (een lichte vorm van de *'bouwsteenmethode'*), namelijk aan de ene kant alles wat te maken heeft met reputatie en aan de andere kant alles wat te maken heeft met het verklaren van het gedrag van organisaties. Tenslotte is er nog een zoekopdracht gedaan die beide deelonderwerpen met elkaar verbindt. In de tabel onder *'Fase 3'* staat weergegeven welke termen precies zijn gebruikt, waarom deze zoektermen zijn gebruikt, het aantal hits wat de zoekterm opbracht en welke vervolgactie eraan zijn gekoppeld. Aangezien reputatie een interessant onderwerp is, wordt de zoekstrategie daar specifiek op gericht.

Fase 2: database, filters en criteria

De zoekopdrachten worden in principe uitgevoerd in Google Scholar en via de universiteitsbibliotheek van de OU. Met name EBSCOHost zal gebruikt worden binnen de universiteitsbibliotheek, omdat deze database het beste aansluit bij het vakgebied van de opleiding. De zoektermen zijn in het Engels aangezien ik ook Engelstalige literatuur wil vinden. De meeste wetenschappelijke artikelen zijn in het Engels en ik hoop hiermee mijn uiteindelijke zoekresultaten te verbeteren. Daarnaast hanteer ik in eerste instantie geen criteria voor jaartal en aantal citaten, omdat ik gebruik wil maken van de *sneeuwbalmethode* en *citatiemethode*. Hierin wil ik mij in beginsel niet laten beperken door jaartallen en aantal citaten, maar het aantal citaten kan mij wel helpen om relevante artikelen sneller te vinden. Ik hang er dus geen criterium aan, maar het gebruik het wel bij het beoordelen van artikelen. De sneeuwbalmethode gebruik ik om de literatuurlijsten te raadplegen van artikelen die ik heb gevonden en die ik relevant acht. De bronnen die daarin zijn gebruikt om het artikel te schrijven, kan ik mogelijk ook voor mijn onderzoek gebruiken. De citatiemethode gebruik ik om artikelen te zoeken die het artikel wat ik heb gevonden en relevant acht, ook citeren.

Fase 3: Zoekresultaten op volgorde van moment:

	Zoektermen	Redenatie voor deze zoekterm	Aantal hits op 01-10-2019	Bruikbaar of niet?
Reputatie	Corporate image and reputation en hieraan gerelateerd organizational reputation	Imago en reputatie zijn begrippen die dicht bij elkaar liggen. Ik wil er meer over lezen in de context van een organisatie en het belang ervan voor organisaties.	739.000 in Google Scholar / 13.893 EBSCO	Ondanks dat deze zoektermen samen veel hits opleveren, blijkt dat de artikelen veel geciteerd worden. Een korte scan van de artikelen die citeren, levert ook relevante literatuur op.

Gedrag van organisaties	Organisational behaviour	Om te weten waarom organisaties dingen wel en niet doen, is het interessant om meer te weten over theorieën die te maken hebben met het gedrag van organisaties.	998.000 Google Scholar / 13.839 EBSCO	Deze zoekvraag levert veel boeken op in EBSCO. Daarom zal ik mij voor deze zoekopdracht meer richten op Google Scholar want daar komen meer papers terug in de resultaten. Wanneer ik organisational vervang door insitutional, komen er relevantere artikelen uit voor mijn onderzoek. Voor vervolg zoekvragen zal ik hier ook rekening mee houden.
Overkoepelende zoektermen	Influence reputation on privacy	De scriptie zal zich richten op privacy, dus het is relevant om te kijken wat de literatuur zegt over privacy in relatie tot reputatie.	639.000 in Google Scholar / 4 EBSCO	Deze hit levert in eerste instantie geen artikelen die direct bruikbaar zouden kunnen zijn. Hierop moet een van de methodes toegepast worden.
	influence privacy organization ->	De scriptie zal zich richten op privacy, dus het is relevant om te kijken wat de literatuur zegt over het gedrag van organisaties in relatie tot privacy.	3050.000 in Google Scholar / 4 EBSCO	EBSCO levert niet direct relevante artikelen op. Google Scholar wel, maar ook hier moeten nog extra methodes worden toegepast.

	organisational behaviour and reputation	De scriptie zal zich richten op het gedrag van organisaties en reputatie, dus het is relevant om te kijken wat de literatuur zegt over het gedrag van organisaties in relatie tot reputatie.	154.000 in Google Scholar / 1042 in EBSCO	Het blijkt dat de resultaten veel ruis opleveren. Om achter artikelen te komen zal ik de eerste zoekvraag via de citatiemethode verder worden toegespitst.
	Substantive implementation	Om te kijken hoe andere onderzoeken zijn uitgevoerd die zich ook richten op substantive en symbolic implementatie is het goed om daar ook nog literatuur over te vinden, meer om een idee te krijgen van het doen van dergelijk onderzoek.	821.000 in Google Scholar / 236 in EBSCO	Om te kijken hoe andere onderzoeken zijn uitgevoerd die zich richten op symbolic en substantive beleid, is het interessant om hier ook een zoekvraag over op te zetten. De resultaten zijn op het eerste oog zeer bruikbaar.
	Privacy Cookies	Ik wil mijn onderzoek specifiek richten op cookies, dus het is interessant om artikelen te vinden die onderzoek hebben gedaan naar cookies en de relatie met privacy	2.110.000 in Google Scholar.	Op het eerste gezicht zijn er voldoende artikelen die gebruikt kunnen worden voor een eerste scan.

Fase 4: selectie van relevante artikelen

Nadat ik bovenstaande zoekopdrachten heb uitgevoerd, ben ik tot een aantal artikelen gekomen die ik als basis zie voor mijn theoretisch kader. Deze artikelen zijn allen gevonden via de sneeuwbalmethode of de citatiemethode.

In onderstaande tabel staat een overzicht van deze basisartikelen. Per artikel staat aangegeven via welke methode deze is gevonden en welke relevante literatuur eraan gelinkt is, als je zowel de '***snowball' methode*** als de ***citatiemethode*** zou toepassen. Het is niet uitgesloten dat er gaandeweg het schrijven van het theoretisch kader, nog artikelen aan toe zijn gevoegd, indien blijkt dat er over een bepaald onderwerp toch meer wetenschappelijke onderbouwing nodig is. Dit zal dan echter geen basisartikel zijn zoals onderstaande, maar meer een artikel voor wat extra body.

TITEL ARTIKEL EN AUTEUR	GEVONDEN VIA	RELEVANTIE
1) An Examination of Differences Between Organizational Legitimacy and Organizational Reputation (Deephouse & Carter, 2005)	Dit artikel heb ik gevonden door middel van de eerste zoekopdracht, het was meteen de eerste hit op Google Scholar. Dit artikel ga ik gebruiken om via de 'snowball' methode en de citatenmethode relevante en aan dit onderzoek gerelateerde artikelen te vinden.	Op 01/10/2019 is het artikel 1.117 keer geciteerd. Het artikel gaat in op de relatie tussen reputatie en legitimiteit. Legitimiteit is belangrijk omdat dat impact heeft op organisatietheorieën, met name op de institutionele theorie, de resource dependence theorie en de organizational ecology theorie. Organisatietheorieën zijn voor mij relevant omdat die kunnen helpen bij het verklaren van het gedrag van organisaties. Dankzij dit artikel werd ik ook gewezen op het concept van legitimiteit, wat dus gerelateerd is aan reputatie.
2) Institutionalized organizations: Formal structure as myth and ceremony (Meyer & Rowan, 1977)	Citatiemethode. Het artikel wordt namelijk in artikel 1 als 'grounded theory' gebruikt.	Op 01/10/2019 is het artikel van Meyer en Rowan 31.159 keer geciteerd en dus zeer goed is ingebed in de wetenschappelijke literatuur. Het gaat specifiek in op de institutionele theorie. Via de sneeuwbalmethode zal ik verder zoeken naar relevante artikelen die hierop doorgaan. Het interessante aan deze institutionele theorie, is dat die ook gebruikt kan worden om het gedrag van organisaties te verklaren voor zaken die niet per definitie in het belang zijn voor de organisatie (zoals een 'opgelegde AVG').
3) What's in a Name? Reputation Building and Corporate Strategy (Fombrun & Shanley, 1990)	Dit artikel heb ik gevonden door in Google Scholar de 'snowball' methode toe te passen op artikel 2. Ik heb gezocht op artikelen dit artikel 2 hebben geciteerd, toegespitst met de zoekopdracht van organizational reputiation.	Op 02/10/2019 is dit artikel 6.232 keer geciteerd. Dit artikel gaat in op de relevantie van reputatie en de relatie tussen reputatie en het gedrag van organisaties. Dit artikel legt dus heel mooi de link tussen mijn onderzoeksgebied, namelijk de relatie tussen het gedrag van organisaties (substantive of symbolic) en reputatie.
4) Rethinking the Relationship Between Reputation and Legitimacy: A Social Actor Conceptualization (King & Whetten, 2008)	Dit artikel heb ik gevonden door op artikel 1 de 'snowball' methode toe te passen. In Google Scholar heb ik heb ik dat gedaan, samen met de zoekvraag over reputatie.	Dit artikel heeft op 02/10/2019, 348 citaten. Dat zijn er niet veel vergeleken met andere artikelen, maar het is wel een voldoende aantal om er van uit te gaan dat het een betrouwbaar artikel is. Dit artikel beschrijft niet de verschillen tussen reputatie en legitimiteit (zoals in artikel 1), maar juist de relatie tussen beide.
5) Strategic responses to institutional processes (Oliver, 1991)	Dit artikel heb ik gevonden via de citatiemethode. In artikel 4 wordt dit artikel namelijk aangedragen als basisartikel. Daarnaast verwijs dit artikel ook weer naar artikel 2.	Dit artikel is op 02/10/2019 9.567 keer geciteerd. Dit artikel gebruik ik om mij extra te verdiepen in de institutionele theorie en omdat hier ook de link wordt gelegd met legitimiteit past dit artikel heel mooi bij de andere.
6) When the bureaucrat promises to safeguard your online privacy: Dissecting the contents of privacy statements on Dutch municipal websites. (Beldad, De Jong, & Steehouder, 2009)	Dit artikel heb ik gevonden via een omweg gevonden. Toen ik de zoekopdacht deed voor privacy en cookies, kwam ik een artikel tegen met de titel:	Dit artikel is slechts 18 keer geciteerd, op 04-10-2019. Dat is niet veel, maar op zich wel te verklaren aangezien het een artikel is die zich op een zeer specifieke case richt. Het artikel is bruikbaar omdat ze onderzoek hebben gedaan naar online

		The EU e-privacy directive: a monstrous attempt to starve the cookie monster?. Dit artikel zelf was niet bruikbaar, maar ik heb wel gekeken door welke andere artikelen, dit artikel werd geciteerd. Het artikel van Beldad en anderen, kwam hierdoor naar boven en dus via de 'snowball' methode.	privacy statements bij de Nederlandse overheid en ook hebben gekeken naar online profiling.
7)	Trustmarks, Objective-Source Ratings, and Implied Investments in Advertising: Investigating Online Trust and the Context-Specific Nature of Internet Signals. (Aiken & Boush, 2006)	In artikel 6 wordt dit artikel als bron aangehaald. Ik heb dit artikel dus gevonden via de citatiemethode.	Op 04-10-2019 is dit artikel 270 keer geciteerd. Dit onderzoek gaat in op de invloed van de aanwezigheid van trustmarks op het vertouwen van consumenten in bedrijven.
8)	Beyond concern—a privacy-trust-behavioral intention model of electronic commerce. (Liu et al., 2005)	In artikel 6 wordt dit artikel als bron aangehaald. Ik heb dit artikel dus gevonden via de citatiemethode.	Op 04-10-2019 is dit artikel 498 keer geciteerd. Dit artikel is relevant voor mijn onderzoek, aangezien ze in dit artikel specifiek ingaan welke factoren het vertrouwen van mensen beïnvloed in online bedrijven in relatie tot privacy.
9)	Managing legitimacy: Strategic and institutional approaches (Suchman, 1995)	Voor dit artikel heb ik een andere zoekopdracht gehanteerd dan hierboven staat beschreven, omdat ik merkte dat ik hierdoor toch nog een link miste in het onderzoek. Ik heb apart gezocht op: legitimacy institutional theory.	Op 06-10-2019 is het artikel 14.709 keer geciteerd. Dit artikel gebruik ik om de link tussen legitimiteit en de institutionele theorie te leggen.
10)	An Integrative Model of Organizational Trust (Mayer et al., 1995)	Dit artikel wordt door artikel 8 aangehaald en heb ik dus gevonden via de citatiemethode.	Op 12-10-2019 is het artikel 20.467 keer geciteerd. Dit artikel wordt veel aangehaald als het gaat om e-commerce en vertrouwen en kan daarmee gezien worden als een van de bron artikelen die over dit onderwerp gaan.

Bijlage 2: Bepaling benodigd aantal respondenten

Om het aantal respondenten te kunnen bepalen, dienen er een aantal berekeningen gedaan te worden. In deze bijlage worden de berekeningen onderbouwd en visueel weergegeven.

Aantal scenario's
Allereerst is het belangrijk om het aantal scenario's te bepalen die in het onderzoek voorkomen. In tabel 28 is te zien dat iedere variabele, twee opties heeft. Het totaalaantal scenario's komt dan uit op 2x2x2=8 scenario's.

Tabel 28: bepaling aantal scenario's

Hypothese / variabele	Aantal opties
Hypothese 1: trustmarks	Variant 1: een vorm met zichtbare trustmark Variant 2: een vorm zonder zichtbare trustmark
Hypothese 2: inhoudelijke privacy policy	Variant 1: een vorm met een inhoudelijk goede privacy policy Variant 2: een vorm met een inhoudelijk minder goede privacy policy
Hypothese 3: data protection officer (DPO)	Variant 1: een vorm waarin een (een goede) DPO aanwezig is Variant 2: een vorm waarin een minder goede DPO aanwezig is
Totaal	Totaal: 2x2x2=8 scenario's

Aantal respondenten
Indien ieder scenario beantwoord zou worden door unieke respondenten, en je uitgaat van het optimale aantal van 30 respondenten per variant, zou je 60 respondenten nodig hebben. In paragraaf 3.3.2 is uitgelegd hoe de berekening van deze 60 respondenten tot stand is gekomen. Rekening houdend met een gewenst betrouwbaarheidsniveau van 95%, een foutmarge van 5% maar een reactiepercentage van ongeveer 50% aangezien de 'convenience sampling' methode gehanteerd wordt, betekent dit dat de vraag bij tenminste 100 personen uitgezet zal worden. Ook is overwogen om iedere respondent, vragen over meerdere scenario's te laten beantwoorden in plaats van één. In dat geval zou je meer data kunnen verzamelen met de helft minder respondenten. Echter heeft deze strategie niet de voorkeur, omdat respondenten in dat geval mogelijk niet meer zo objectief zijn bij het beantwoorden van de tweede set aan vragen, aangezien ze ook al andere varianten hebben gezien. In de gekozen methode weet de respondent niet dat er andere scenario's zijn waardoor de beantwoording van de vragen vermoedelijk objectiever zal zijn.

In tabel 29 wordt weergegeven hoe de berekening tot stand is gekomen dat iedere variabele, vier keer voorkomt in de acht scenario's. In onderstaande tabel corresponderen de getallen met de varianten in tabel 28.

Tabel 29: overzicht indeling scenario's

	VARIABELE TRUSTMARK	VARIABELE PRIVACY POLICY	VARIABELE DPO	BEOOGD AANTAL RESPONDENTEN	FEITELIJK AANTAL RESPONDENTEN
SCENARIO					
1	1	1	1	7,5	11
2	1	1	2	7,5	7 (was 8)
3	1	2	2	7,5	9 (was 10)
4	2	1	2	7,5	12
5	2	2	1	7,5	12
6	2	1	1	7,5	8
7	1	2	1	7,5	9
8	2	2	2	7,5	11
TOTAAL	1 komt 4 keer voor 2 komt 4 keer voor	1 komt 4 keer voor 2 komt 4 keer voor	1 komt 4 keer voor 2 komt 4 keer voor	_____+ =60 respondenten	_____+ =79

Om dus te kunnen bepalen hoeveel respondenten er voor dit onderzoek nodig zijn, is 30 (het optimale aantal respondenten per variant) gedeeld door vier (het aantal keer dat de variant voorkomt in de scenario's) wat uitkomt op 7,5. Dat is vermenigvuldigd met het aantal scenario's (acht scenario's) wat uitkomt op een totaal van optimaal 60 respondenten. De laatste kolom geeft weer hoeveel respondenten er per scenario feitelijk zijn gehaald na het afnemen van de vragenlijst en na het uitvoeren van de analyses op de betrouwbaarheid van de antwoorden van de respondenten. Op basis van die laatste controle is er bij scenario 2 en 3 een respondent weggevallen. Het gevolg hiervan is dat voor scenario 2 niet meer het voldoende aantal respondenten behaald.

Bijlage 3: Ontwikkelen van de enquête

Om de enquête zo goed mogelijk uit te voeren zijn er keuzes gemaakt met betrekking tot de opzet. In deze bijlage wordt besproken welke keuzes zijn gemaakt en waarom die zijn gemaakt. Bijvoorbeeld de keuze voor bepaalde vragen, de manier waarop de scenario's zijn voorgelegd en de manier van verspreiden.

Stap 1: Vaststellen van de scenario's

Per variabele zijn er twee opties die voorgelegd kunnen worden. In bijlage 2 is uitgelegd hoe dit in het onderzoek wordt toegepast. In deze paragraaf worden de opties weergegeven en wordt besproken hoe de omschrijving tot stand is gekomen.

Variabele 1: Trustmark

Als tweede variabele wordt een van de onderstaande varianten van een trustmark getoond. Er is gebruik gemaakt van een willekeurige website, in dit geval die van Etos, waarbij het gemakkelijk was om de site te manipuleren zodat het niet meer duidelijk is van welk bedrijf de site is en waarbij het makkelijk is om verschillende varianten te maken.

Variant 1: Afbeelding met trustmark

Variant 2: Afbeelding zonder trustmark

Variabele 2: privacy policy

Voor het opstellen van een beschrijving van een privacy policy is gekozen om de uitkomsten van het onderzoek van Wu et al. (2012) te gebruiken om de verschillende varianten vorm te geven. Uit hun onderzoek blijkt namelijk waar een goede privacy policy aan moet voldoen. Er zijn een vijftal elementen onderzocht die van positieve invloed blijken te zijn (Wu et al., 2012):

1) Notice – The website discloses what personal information is going to be collected;
2) Access – The website allows you to review collected personal information;
3) Security – The website explains that the domain takes some steps to provide security for personal information has been collected;
4) Choice – The website informs whether personal information will be disclosed to a third party and explains under what conditions;
5) Enforcement – The website discloses that there is a law sanctioning those who violate the privacy statement.

In variant 1 zullen deze elementen meegenomen worden, in variant 2 worden deze elementen niet meegenomen maar worden andere elementen getoond. Voor variant 1 is gekozen om een privacy policy te genereren via www.veiliginternetten.nl. De Autoriteit Persoonsgegevens raadt aan om via deze website een goede privacy policy te genereren. Voor variant 2 is een privacy policy gemanipuleerd die standaard wordt gebruikt door gemeentes, naar een privacy policy die niet voldoet aan de hierboven genoemde elementen. Deze policy's zijn verkort en alleen essentiële elementen zijn eruit gehaald en gepresenteerd aan de respondenten. Te veel tekst zou ervoor kunnen zorgen dat respondenten vroegtijdig afhaken vanwege de lengte van de vragenlijst.

Variant 1: Goede privacy policy:

Contactgegevens
Bedrijf x, gevestigd aan Bedrijf X Postbus 1234 1234AA Voorbeeld, is verantwoordelijk voor de verwerking van persoonsgegevens zoals weergegeven in deze privacyverklaring. Dhr. V. Oorbeeld is de Functionaris Gegevensbescherming van Bedrijf x. Hij is te bereiken via v.oorbeeld@bedrijf-x.nl

Persoonsgegevens die wij verwerken
Bedrijf x verwerkt uw persoonsgegevens doordat u gebruik maakt van onze diensten en/of omdat u deze zelf aan ons verstrekt. Hieronder vindt u een overzicht van de persoonsgegevens die wij verwerken:
- Voor- en achternaam
- Geslacht
- IP-adres
- Internetbrowser en apparaat type

Gegevens inzien, aanpassen of verwijderen
U heeft het recht om uw persoonsgegevens in te zien, te corrigeren of te verwijderen. Daarnaast heeft u het recht om uw eventuele toestemming voor de gegevensverwerking in te trekken of bezwaar te maken tegen de verwerking van uw persoonsgegevens door Bedrijf x en heeft u het recht op gegevensoverdraagbaarheid. U kunt een verzoek tot inzage, correctie, verwijdering, gegevensoverdraging van uw persoonsgegevens of verzoek tot intrekking van uw toestemming of bezwaar op de verwerking van uw persoonsgegevens sturen naar hallo@bedrijf-x.nl.

Hoe wij persoonsgegevens beveiligen
Bedrijf x neemt de bescherming van uw gegevens serieus en neemt passende maatregelen om misbruik, verlies, onbevoegde toegang, ongewenste openbaarmaking en ongeoorloofde wijziging tegen te gaan. Bedrijf x heeft de volgende maatregelen genomen om uw persoonsgegevens te beveiligen:
- Beveiligingssoftware, zoals een virusscanner en firewall.
- TLS (voorheen SSL) Wij versturen uw gegevens via een beveiligde internetverbinding. DNSSEC is een extra beveiliging (aanvullend op DNS) voor het omzetten van een domeinnaam naar het hieraan gekoppelde IP-adres.

Delen van persoonsgegevens met derden
Bedrijf x deelt uw persoonsgegevens met verschillende derden als dit noodzakelijk is voor het uitvoeren van de overeenkomst en om te voldoen aan een eventuele wettelijke verplichting. Met bedrijven die u gegevens verwerken in onze opdracht, sluiten wij een bewerkersovereenkomst. Bedrijf x blijft verantwoordelijk. Daarnaast verstrekt Bedrijf x uw persoonsgegevens aan andere derden alleen met uw nadrukkelijke toestemming.

Sancties voor het niet naleven van de privacy policy
Bedrijf x hanteert strikte regels om uw gegevens veilig en op een goede manier te verwerken. Ongeautoriseerde toegang en misbruik van uw gegevens door onze medewerkers, wordt bestraft en altijd gevolgd door aangifte bij de politie en een melding bij de Autoriteit Persoonsgegevens.

Variant 2: Minder goede privacy policy:

Contactgegevens
Bedrijf x, gevestigd aan Bedrijf X Postbus 1234 1234AA Voorbeeld, is verantwoordelijk voor de verwerking van persoonsgegevens zoals weergegeven in deze privacyverklaring. Dhr. V. Oorbeeld is de Functionaris Gegevensbescherming van Bedrijf x. Hij is te bereiken via v.oorbeeld@bedrijf-x.nl

Bewaartermijn
Bedrijf x bewaart uw persoonsgegevens niet langer dan nodig is voor de goede uitvoering van haar taken en de naleving van de wettelijke verplichtingen.

Bijzondere en/of gevoelige persoonsgegevens die wij verwerken
Onze website heeft niet de intentie gegevens te verzamelen over websitebezoekers die jonger zijn dan 16 jaar. Tenzij ze toestemming hebben van ouders of voogd. We kunnen echter niet controleren of een bezoeker ouder dan 16 is.

Gebruik van het platform
www.bedrijf-x.nl kan linken naar websites van anderen. Bedrijf x is niet verantwoordelijk voor de naleving van de privacywet- en regelgeving door deze derden.

Wijziging verklaring inzake Gegevensbescherming
Deze verklaring inzake Gegevensbescherming kan, zonder waarschuwing, door Bedrijf x gewijzigd worden. Deze wijzigingen treden in werking vanaf het moment dat ze op www.bedrijf-x.nl gepubliceerd zijn.

Telefoon-, WhatsApp- en chatgesprekken
Telefoon-, WhatsApp- en chatgesprekken kunnen door Bedrijf x worden bewaard om de dienstverlening te verbeteren. Gesprekken worden niet langer bewaard dan nodig is.

Variabele 3: DPO

Er is nog geen literatuur beschikbaar waaraan een goede Data Protection Officer moet voldoen. Daarom is gekeken naar de eisen in twee willekeurige openstaande vacatures voor deze positie en via LinkedIn gekeken naar twee profielen van mensen die op dit moment deze functie vervullen. In onderstaande tabel is deze analyse schematisch weergegeven.

	VACATURE 1: INOCARE UTRECHT	VACATURE 2: CUCCIBU B.V.	PROFIEL LINKEDIN 1: WILKE UYTDEHAAGE	PROFIEL LINKEDIN 2: MARTIN VAN RIJSWIJK
AANTAL JAAR RELEVANTE WERKERVARING	3-4 jaar	3-5 jaar	18 jaar	9 jaar
OPLEIDING	Juridische WO opleiding	Een afgeronde HBO of WO-opleiding met één of meer van de volgende componenten: Bedrijfskunde, Organisatiekunde, Rechten of Management.	Rechten (WO)	Commerciële Economie (HBO)
AANVULLENDE CURSUSSEN	Opleiding tot Functionaris Gegevensbescherming	Opleiding CIPP/e, CIPM of CIPT.	IIR, opleiding Certified data protection officer (CDPO)	Specialisatie-opleiding Functionaris Gegevens-bescherming (ICTRecht)

Op basis van bovenstaande profielkenmerken is een profiel gemaakt wat hier goed aan zou voldoen en een profiel wat hier niet goed aan voldoet. Dit profiel is ook getoetst aan de kenmerken die de Autoriteit Persoonsgegevens verbindt aan een goede Functionaris

Gegevensbescherming. Beide varianten zijn in een CV uitgewerkt welke aan de respondenten voorgelegd gaan worden.

Variant 1: DPO die aan bovenstaande kenmerken voldoet

Curriculum Vitae

Persoonsgegevens
Naam: Victor Oorbeeld
Telefoonnummer: 06-12345678
Rijbewijs: A & B

Opleidingsachtergrond

1990 – 1995	*Zuid-Holland College*	VWO
1995 – 1998	*Universiteit van Zuid-Holland*	Bachelor Rechten
1998 – 2000	*Universiteit van Zuid-Holland*	Master Rechten (Privacy recht)

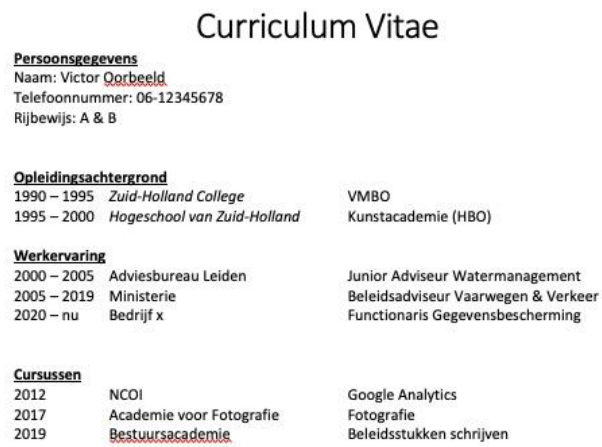
Werkervaring

2000 – 2005	Adviesbureau Leiden	Privacy jurist
2005 – 2015	Adviesbureau Utrecht	Adviseur persoonsgegevens en data
2015 – nu	Bedrijf x	Functionaris Gegevensbescherming

Cursussen

2012	IMF Academy	Certified Information Privacy Professional/Europe
2017	ICT&Recht	Specialisatieopleiding Functionaris Gegevensbescherming
2019	IMF Academy	Certified Information Privacy Manager

Variant 2: DPO die niet aan bovenstaande kenmerken voldoet



Curriculum Vitae

Persoonsgegevens
Naam: Victor Oorbeeld
Telefoonnummer: 06-12345678
Rijbewijs: A & B

Opleidingsachtergrond

1990 – 1995	*Zuid-Holland College*	VMBO
1995 – 2000	*Hogeschool van Zuid-Holland*	Kunstacademie (HBO)

Werkervaring

2000 – 2005	Adviesbureau Leiden	Junior Adviseur Watermanagement
2005 – 2019	Ministerie	Beleidsadviseur Vaarwegen & Verkeer
2020 – nu	Bedrijf x	Functionaris Gegevensbescherming

Cursussen

2012	NCOI	Google Analytics
2017	Academie voor Fotografie	Fotografie
2019	Bestuursacademie	Beleidsstukken schrijven

Stap 2: Vaststellen van de vragen na het bekijken van de scenario's
In totaal zijn er acht verschillende scenario's en dus ook acht verschillende enquêtes. De vragen die gesteld worden in de enquêtes, zijn voor alle acht enquêtes gelijk. De scenario's zijn vanzelfsprekend verschillend. Hierdoor wordt precies gemeten wat de invloed is van de verschillende onderdelen van een scenario op de beantwoording van de vragen van de respondenten. Om de vragen te bepalen is gebruikgemaakt van een aantal verschillende, reeds uitgevoerde, onderzoeken wat de betrouwbaarheid van de vragen verhoogt. De vragen waarmee vertrouwen wordt gemeten na ieder scenario, komen uit de onderzoeken van Hong en Cho (2011), McKnight et al. (2002a) en Yang, Lin, Chandlrees, en Chao (2009). Er is gekozen voor deze onderzoeken omdat ze allen de vragenlijst al in het artikel hebben staan waardoor deze direct beschikbaar. Daarnaast zijn deze onderzoeken gerelateerd zijn aan het onderwerp van dit onderzoek en gebruiken ze dezelfde concepten van vertrouwen als de concepten in dit onderzoek. Tenslotte hebben deze onderzoeken wetenschappelijk onderbouwd hoe ze tot

deze vragen zijn gekomen en hebben ze statistische analyses beschikbaar gesteld waaruit de betrouwbaarheid van de vragen blijkt. Tussen de onderzoeken heeft een crosscheck plaatsgevonden om te kijken welke vragen (enigszins) overlap hadden en welke van hun vragen ook bruikbaar zijn voor dit onderzoek. Indien een vraag niet bruikbaar is voor dit onderzoek, is dat ook verantwoord. Alleen de vragen, waaruit bleek in deze onderzoeken dat ze voldoende betrouwbaar waren, en die de verschillende concepten van vertrouwen meten die ook in dit onderzoek voorkomen, zijn overwogen voor dit onderzoek. In onderstaande tabel is de totstandkoming visueel weergegeven. Groen geeft aan dat de vragen gerelateerd zijn aan elkaar, oranje geeft aan dat de vragen (te veel) van elkaar afwijken dat ze als verschillende vragen dienen te worden beschouwd. Vanzelfsprekend zijn de vragen vertaald naar het Nederlands en dusdanig geformuleerd dat ze aansluiten bij dit onderzoek.

Concept van vertrouwen	**Vraag gebruikt in onderzoek van Hong en Cho (2011)**	**Vraag gebruikt in artikel van McKnight et al. (2002a).**	**Vraag gebruikt in artikel van Yang, Lin en Chao (2009)**
Competence-based trust	I think that this Website has the necessary abilities to carry out its work.	LegalAdvice.com is competent and effective in providing legal advice.	Geen gerelateerde vraag in dit onderzoek.
	I think that this Website has sufficient experience in the marketing of the products and services that it offers.	LegalAdvice.com performs its role of giving legal advice very well.	Shop.com performs its role of giving fulfillment of any transaction carried out.
	I think that this Website has the necessary resources to carry out its activities successfully.	Overall, LegalAdvice.com is a capable and proficient Internet legal advice provider.	In general, Shop.com is very capable in handling online transactions.
	I think that this Website knows its users well enough to offer them products and services adapted to their needs.	In general, LegalAdvice.com is very knowledgeable about the law.	Geen gerelateerde vraag in dit onderzoek.
Integrity-based trust	I think that this Website usually fulfills the commitments it assumes.	LegalAdvice.com would keep its commitments.	Shop.com would keep its commitments.
	I think that the information offered by this site is sincere and honest.	I would characterize LegalAdvice.com as honest.	I would characterize the Shop.com as honest.
	Geen gerelateerde vraag in dit onderzoek.	LegalAdvice.com is sincere and genuine.	Shop.com is sincere and genuine.
	I think I can have confidence in the promises that this Website makes.	LegalAdvice.com is truthful in its dealings with me.	Shop.com is truthful in its dealings with me.
Institution-based trust	Even if not monitored, I'd trust the intermediary (e.g. internet) to do the job right.	I feel that most Internet vendors would act in a customers' best interest.	Geen gerelateerde vraag in dit onderzoek.
	I trust the intermediary (e.g. internet)	I am comfortable making purchases on the Internet.	Geen gerelateerde vraag in dit onderzoek.

I believe that the intermediary (e.g. internet) is trustworthy.	I feel good about how things go when I do purchasing or other activities on the Internet.	Geen gerelateerde vraag in dit onderzoek.

Daarnaast zijn er ook nog een aantal vragen meegenomen in de enquête die relevant zijn specifiek voor dit onderzoek en daarin uniek vergeleken met andere onderzoeken. Het gaat om de volgende twee vragen:

- Deze organisatie is een voorbeeld voor andere organisaties op het gebied van privacy.
- Deze organisatie gaat goed om met mijn persoonsgegevens.

Stap 3: Bepalen van de manier van meten

De enquête wordt opgebouwd uit stellingen. Respondenten kunnen aangeven in welke mate ze het met de stelling eens of oneens zijn. Er is gekozen voor stellingen omdat dat in de andere onderzoeken ook wordt gehanteerd. Deze vorm van vragen stellen wordt namelijk vaak gebruikt om meningen van respondenten in kaart te brengen. De Likert schaal is hiervoor vaak een veel gebruikte manier, waarbij meestal een indeling van 5 of 7 punten wordt gehanteerd (Saunders et al., 2016, p. 458). Voor dit onderzoek wordt een 6-punts schaal gebruikt met de waardes: sterk mee oneens, mee oneens, een beetje mee oneens, een beetje mee eens, mee eens en sterk mee eens.

Er is gekozen voor een 6-punts schaal vanwege verschillende redenen. Wanneer er te weinig antwoord opties worden aangeboden, wordt het moeilijk om onderzoek te doen naar de daadwerkelijke houding van een respondent ten opzichte van het onderwerp (S.-H. Kim, 2010). Een Likertschaal wordt daarnaast statistisch betrouwbaarder, naarmate de spreiding van de opties hoger is (Jacoby & Matell, 1971). Wat de ultieme schaal is, volgens wetenschappelijke onderzoeken lastig te bepalen. Naast een minimum, zit er namelijk ook een maximum aan het aantal punten wat aan een respondent wordt aangeboden (Sparling & Sen, 2010). Wat dat maximum is, verschilt per onderzoek. Volgens bijvoorbeeld Sparling en Sen (2010) ligt dat bij 5 punten, maar volgens het onderzoek van Preston en Colman (2000) bijvoorbeeld bij een 10-punts schaal gevolgd door een schaal van 7 punten en van 9 punten. Kortom, de meningen verschillen over de lengte, maar deze ligt ergens tussen de 5 en de 10 punten. Meningen verschillen ook over een even of oneven aantal punten. Het onderzoek van Jacoby en Matell (1971) onderschrijft bijvoorbeeld het belang van een even schaal, omdat dan het middelpunt ontbreekt. Terwijl het onderzoek van Garland (1991) juist aangeeft dat het gebruik van een middelpunt context afhankelijk is waardoor de onderzoeker zelf een afweging moet maken of een middelpunt al dan niet toegevoegd wordt. Daarnaast hebben Chyung, Roberts, Swanson, en Hankinson (2017) in hun onderzoek reeds beschikbare onderzoeken bekeken over het al dan niet toevoegen van een middelpunt en de lengte van de schaal. De conclusie van hun onderzoek is vergelijkbaar met bovenstaande analyse, namelijk dat er eigenlijk geen duidelijke conclusie is en dat het antwoord gezocht moet worden in het onderzoek zelf. Daarom is er geprobeerd om ook te kijken naar de schaalverdeling van andere wetenschappelijke onderzoeken die een soortgelijk experiment hebben uitgevoerd. Echter blijken ook deze onderzoeken niet eenduidig te zijn of er wordt in de onderzoeken niet vermeld wat de gebruikte schaalverdeling is geweest.

Om uiteindelijk toch een keuze te kunnen maken is uitgegaan van het idee dat de statistische analyse betrouwbaarder wordt naar mate er meer punten zijn, zoals wordt genoemd in het

onderzoek van S.-H. Kim (2010) en Jacoby en Matell (1971), want daarover lijkt de wetenschap het in de basis wel eens te zijn. Ook is ervoor gekozen om de gedachte te volgen om geen middelpunt toe te voegen tenzij er redenen zijn om aan te nemen dat dat relevant zou kunnen zijn voor het onderzoek (Chyung et al., 2017). Voor dit onderzoek zijn die redenen er niet en kan het, vanwege het experimentele karakter, juist gewenst zijn om respondenten te dwingen een 'kant' te kiezen. Om vervolgens te bepalen of het dan een 4, 6 of 8 punt schaal zou moeten worden is er gekeken naar de onderzoeksopzet waarbij het aantal respondenten op optimaal 7,5 per scenario is vastgesteld, zoals wordt besproken in bijlage 2. Om te voorkomen dat de variatie binnen deze relatief kleine groep te groot of te klein wordt, bij bijvoorbeeld 4 punten of 8 punten, is er gekozen om voor de middenweg te kiezen en de 6-punts schaal toe te passen. Ook deze keuze is weer gebaseerd op eerdere literatuur. Er is bijvoorbeeld door Chomeya (2010) onderzoek gedaan naar welke schaal beter is voor psychologische testen, bijvoorbeeld testen over iemands houding ten opzichte van een onderwerp: een 5-punts of een 6-punts schaal? Uit dit onderzoek bleek dat een 6-punts schaal in alle opzichten betere resultaten opleverde op het gebied van construct validiteit, discriminatie, en betrouwbaarheid. Ook uit een ander onderzoek van Hills en Argyle (2002) en Leung (2011) blijkt dat de 6-punts schaal als betrouwbaar meetinstrument gezien kan worden in vergelijking met een 4, 5 of 11 punt schaal. Al deze onderzoeken samen hebben uiteindelijk geleid tot de keuze voor een 6-punt schaal.

Voor dit onderzoek zijn de vragen geplaatst in een enquête tool. Van de acht verschillende vragenlijsten wordt aan een respondent één vragenlijst random toegewezen. Hiermee wordt bias vanuit de onderzoeker voorkomen. In de volgende stap wordt de opbouw van de enquête uitvoeriger besproken en wordt de 6-punt schaal toegepast op de gekozen vragen.

Stap 4: Vormgeven van de enquête
In deze fase wordt de enquête vormgegeven en gereed gemaakt voor publicatie. De opzet zit er als volgt uit:

Pagina van de enquête	**Doel**	**Opmerkingen**
1: Welkom	De respondent van relevante informatie vooraf voorzien zoals de naam van de onderzoeker, het doel van het onderzoek en wat privacy maatregelen.	Er wordt beschreven dat de data 10 jaar wordt bewaard, dat een respondent zich altijd terug kan trekken uit het onderzoek en dat antwoorden nooit op persoonsniveau te herleiden zijn. Ook wordt een e-mailadres gedeeld voor het geval er vragen zijn.
2: Introductie van de drie verschillende beschrijvingen	De respondent uitleggen dat er drie verschillende beschrijvingen volgen en dat ze deze aandachtig dienen te lezen.	
3, 4 & 5: Beschrijving van de variabelen	Op deze pagina's worden de verschillende beschrijvingen van de variabelen getoond.	Per variabele wordt één van de twee varianten getoond. Deze varianten zijn te vinden aan het begin van deze bijlage.
6: Stellingen over vertrouwen	1) De organisatie komt over als een betrouwbare organisatie. 2) De informatie die deze organisatie aanbiedt is eerlijk en transparant.	Respondenten hebben de keuze uit de antwoorden: Helemaal mee oneens, mee oneens, een beetje mee oneens, een beetje mee eens, mee eens of helemaal mee eens.

	3) Deze organisatie heeft kennis van zaken. 4) Als ik bij deze organisatie iets zou bestellen, zou ik er vertrouwen in hebben dat het geleverd wordt. 5) Deze organisatie gaat goed om met mijn persoonsgegevens. 6) Ook als niemand het zou monitoren, zou deze organisatie nog het goede doen. 7) Deze organisatie is een voorbeeld voor andere organisaties op het gebied van privacy. 8) De organisatie komt geloofwaardig op mij over.	
7: Achtergrond vragen	1) Over het algemeen heb ik er vertrouwen in dat het kopen van producten goed gaat als ik ze aanschaf via internet. 2) Ik voel mij comfortabel bij het doen van aankopen op het internet. 3) In de meeste gevallen komen online verkopers hun afspraken na. 4) Over het algemeen heb ik positieve ervaringen met het doen van online aankopen. 5) Ik zie mijzelf als (helemaal niet ervaren/een beetje ervaren/ervaren/heel erg ervaren) met het doen van aankopen via internet. 6) Ik vind het (helemaal niet belangrijk/een beetje belangrijk/belangrijk/heel erg belangrijk) hoe organisaties omgaan met mijn persoonsgegevens. 7) In welke leeftijdscategorie val je? 8) Ik ben een man/vrouw/anders & wil niet zeggen.	Respondenten hebben bij de eerste vier vragen de keuze uit de antwoorden: Helemaal mee oneens, mee oneens, een beetje mee oneens, een beetje mee eens, mee eens of helemaal mee eens.
8: Bedankt pagina	De respondent bedanken voor deelname.	

Stap 5: testen van de enquête

Voordat er wordt overgegaan tot publicatie, is de enquête voorgelegd aan een viertal personen die allen in de doelgroep vallen. Aan deze personen is gevraagd om de enquête eenmalig te doorlopen op verschillende apparaten om technisch te controleren of de vragenlijst goed werkt. Tevens is gevraagd aan de respondenten om te letten op zaken als spelfouten, onduidelijkheden, onregelmatigheden, lengte en toegankelijkheid. Hieronder is

een tabel weergegeven per proefpersoon wat de feedback was en wat er met deze feedback is gedaan.

	OPMERKING 1	OPMERKING 2	OPMERKING 3	OPMERKING 4	OPMERKING 5
RESP. 1 (MOBIEL)	Een te lange zin in je inleiding van het onderzoek (de zin die begint met Voor de laatste fase etc.)	De vraag: 'deze organisatie komt beloftes na' vind ik lastig te beantwoorden op basis van de informatie die ik nu heb.	Er zijn meerdere vragen die gelijk zijn aan elkaar maar die anders zijn vormgegeven. Voor de duidelijkheid goed om hier een lijn in te trekken.	Wat is een functionaris gegevensbescherming?	
OPLOSSING	De zin is ingekort.	Deze vraag is geherformuleerd.	Alle vragen die een gelijke opbouw hebben, zijn in dezelfde vorm vormgegeven. Daarnaast zijn er vragen die op elkaar lijken maar die toch een ander doel dienen. Deze vragen zijn ongewijzigd gebleven.	Dit begrip is kort toegelicht op basis van de beschrijving van de Autoriteit Persoonsgegevens.	
RESP. 2 (MOBIEL)	In het begin geef je aan dat gegevens niet naar mij als persoon te herleiden zijn. Misschien handig om extra te benoemen dat invullen zelfs anoniem is?	Het is prettiger om te beginnen met de vragen over jezelf, dan de scenario's te presenteren en dan de vragen over de scenario's te beantwoorden.	De schaalverderling is voor mij onduidelijk.	Ik vind het vervelend dat ik geen midden optie kan kiezen als ik het antwoord niet weet.	
OPLOSSING	Dit is toegevoegd.	Deze opmerking is kritisch overwogen. Toch is ervoor gekozen om hierin geen aanpassing in aan te brengen om twee redenen. Allereerst omdat door het stellen van deze vragen het doel van het onderzoek al te veel wordt verklapt en mensen hierdoor beïnvloed kunnen worden. En als tweede zijn dit de vragen die het minst relevant zijn voor het onderzoek. Als mensen vroegtijdig	De tester had niet gezien dat dit in de vraag was uitgelegd. Maar deze feedback is wel meegenomen en de vormgeving van de Likert-scale is aangepast.	De midden optie is hier niet voor bedoeld. Wel een interessant inzicht dat de literatuur hierin dus gelijk heeft, dat de optie in het midden vaak wel zo wordt gebruikt. Er is overwogen om in plaats van een midden optie 'weet ik niet' toe te voegen. Echter gezien de lage hoeveelheid vragen is dit niet gewenst.	

		afhaken zijn dit de antwoorden die het minst gemist zullen worden.		Het zal meegenomen worden als beperking.	
RESP 3. (LAPTOP)	Ik vond de eerste pagina van de website een beetje onoverzichtelijk door de zwarte vlakken (blijkbaar heb je wat info weg moeten halen).	Bij de pagina's van het privacy statement en de DPO vond ik de fonts wat vreemd. De begeleidende tekst was heel klein, terwijl de inhoud van het statement en het CV heel groot op het scherm kwamen. Dat geeft een wat vreemd beeld.			
OPLOSSING	De zwarte vlakken zijn weggehaald en in plaats daarvan is de tekst verwijderd.	Dat is een technische aanpassing. Dit is nu omgedraaid (afbeelding kleiner, begeleidende tekst groter).			
RESP 4. (LAPTOP)	De introductie vond ik best lang. Dit kan ingekort worden.	De Gemeente Den Haag staat in het privacy statement maar in de CV staat opeens bureau-x.	Deze organisatie komt beloftes na. Dat moet zijn, zijn beloftes.	Bedrijf x --> een echte fictieve naam verzinnen? JoHu BV ofzo?	De instructie los plaatsen van de v.b. Bij het tweede algemene deel van de vragenlijst, heb ik in eerste instantie over de instructie gelezen die erboven stond.
OPLOSSING	De introductie is ingekort.	Dit is aangepast.	Deze vraag is geherformuleerd n.a.v. de feedback van respondent 1.	Omdat bedrijfsnamen allerlei associaties op kunnen roepen, is er bewust voor gekozen om voor een zo neutraal mogelijke variant te kiezen. De bedrijfsnaam wordt niet aangepast.	Dit is aangepast.

Bijlage 4: Overzicht tabellen en statistische testen

In deze bijlage zijn tabellen te vinden die een verdieping laten zien op de statistische analyses die zijn gedaan voor dit onderzoek.

Verdiepende tabellen bij paragraaf 4.3

Factoranalyse

In onderstaande tabel is getoond dat er uit 12 vragen, 2 componenten worden gehaald.

Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	5,979	49,826	49,826	5,979	49,826	49,826	5,658	47,153	47,153
2	2,018	16,818	66,643	2,018	16,818	66,643	2,339	19,490	66,643
3	0,852	7,104	73,747						
4	0,714	5,947	79,694						
5	0,664	5,533	85,227						
6	0,502	4,181	89,409						
7	0,334	2,780	92,189						
8	0,323	2,689	94,878						
9	0,228	1,904	96,782						
10	0,176	1,467	98,249						
11	0,135	1,125	99,375						
12	0,075	0,625	100,000						

Extraction Method: Principal Component Analysis.

Cronbach's Alpha

In onderstaande is weergegeven wat de invloed is van het verwijderen van een bepaalde vraag op de Cronbach's Alpha voor de eerste acht vragen. Indien alle vragen meegenomen worden levert dat een Cronbach's Alpha op van ,941. Alleen met het weghalen van vraag vier zou de Cronbach's Alpha minimaal verhoogd kunnen worden naar ,945. Echter is dit verschil zo minimaal dat er is besloten om dat niet te doen. Het weegt namelijk niet op tegen het verlies aan informatie wat daardoor optreedt.

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
1) De organisatie komt over als een betrouwbare organisatie	25,42	59,810	0,850	0,928
2) De informatie die deze organisatie aanbiedt is eerlijk en transparant	25,34	60,741	0,811	0,931
3) Deze organisatie heeft kennis van zaken	25,56	64,173	0,733	0,936
4) Als ik bij dit bedrijf iets zou bestellen zou ik er vertrouwen in hebben dat het geleverd wordt	25,28	65,306	0,602	0,945
5) Deze organisatie gaat goed om met mijn persoonsgegevens	25,86	57,814	0,856	0,928
6) Ook als niemand het zou monitoren zou deze organisatie nog het goede doen	26,25	62,986	0,766	0,934
7) Deze organisatie is een voorbeeld voor andere organisaties op het gebied van privacy	26,18	59,455	0,811	0,931
8) De organisatie komt geloofwaardig op mij over	25,51	59,740	0,879	0,926

In onderstaande is weergegeven of het weghalen van een van de vragen die propensity (vraag 9 tot en met 12) meten, relevant is om daarmee een hogere Cronbach's Alpha te behalen.

Het blijkt dat dat niet het geval is, in tegendeel want de Cronbach's Alpha wordt daarmee juist verlaagd (alle waardes liggen lager dan 0,726). Er worden daarom geen vragen verwijderd.

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
9) Over het algemeen heb ik er vertrouwen in dat het kopen van producten goed gaat als ik ze aanschaf via internet	14,87	2,907	0,574	0,629
10) Ik voel mij comfortabel bij het doen van aankopen op het internet	14,86	2,737	0,579	0,629
11) In de meeste gevallen komen online verkopers hun afspraken na	14,47	3,509	0,477	0,687
12) Over het algemeen heb ik positieve ervaringen met het doen van online aankopen	14,28	3,998	0,484	0,697

Bepalen normaalverdeling

Het is belangrijk om te weten of er sprake is van een normaalverdeling of niet, aangezien dat bepalend is voor de keuze van de formule voor de analyse. In onderstaande figuren is daarom weergegeven of de verdeling per variant van een variabele normaal verdeeld is of niet. Om dit te bepalen wordt er gekeken naar de resultaten van de Kolmogorov–Smirnovtoets en de Shapiro-Wilktoets. Deze toetsen worden gebruikt om te bepalen of distributie normaal verdeeld is of niet (Field, 2009, p. 144). Indien de p-waarde groter is dan 0,05 betekent het dat de distributie van de sample normaal verdeeld is. Als de p-waarde kleiner is dan 0,05 betekent het dat de distributie van de sample niet normaal verdeeld is.

Een beperking van deze testen wordt vaak gezien bij grote aantallen samples. Echter, daarvan is in dit onderzoek geen sprake en dus zouden de resultaten van deze test betrouwbaar moeten zijn. Tenslotte wordt door onderzoek van Krithikadatta (2014) aangetoond dat een analyse van een normaalverdeling alleen relevant is voor samples boven de n=30. Het maakt voor de normaalverdeling vanaf n=30 of hoger namelijk niet uit hoe groot de populatie is. Onder n=30 heeft een analyse van de normaalverdeling geen zin, omdat de aantallen daarvoor te klein zijn. In dat geval dient er ook altijd gekeken te worden naar de resultaten van non-parametrische testen (Krithikadatta, 2014).